LANDBANK

SERVING THE NATION

SUPPLEMENTAL/BID BULLETIN NO. 1
For LBP-ICTBAC-ITB-GS-20230926-02

PROJECT	:	**Supply, Delivery and Installation of Small Network Firewalls with Three (3) Years Warranty and Support**
IMPLEMENTOR	:	**ICT-BAC Secretariat Unit**
DATE	:	**November 16, 2023**

This Supplemental/Bid Bulletin is issued to modify, amend and/or clarify certain items in the Bid Documents. This shall form an integral part of the Bid Documents.

Modifications, amendments and/or clarifications:

1. The bidder/s are encouraged to use the Bid Securing Declaration as Bid Security.

2. The Terms of Reference (No. 84), Technical Specifications and Checklist of Bidding Documents (Item Nos. 12, 14 and 20 of the Technical Documents) have been revised. Please see attached revised items No.84 and specific sections of the Bidding Documents.

3. Responses to bidder's query/clarifications per attached Annexes H-1 to H-2.

ATTY. KARLA MAY M TEMPOROSA
OIC, ICT-BAC Secretariat Unit

November 15, 2023

Supply, Delivery and Installation for Four (4) Small Network Firewalls with Three years warranty and support – Terms of References

Objective: To *continuously secure and protect the banks network infrastructure against malicious attacks as well as unauthorized ingress and egress network traffic/access.*

	Technical Specifications	Comply?
Hardware Specifications		
1	Must provide Four (4) Hardware built Next Generation Firewall (NGFW) appliances	
2	The proposed Next Generation Security Platform must support 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) and 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	Must have the following interface: • Supports 1xCPUs, 4 Physical cores • Supports 1x240GB SSD Storage • Supports 8GB memory	
6	Must support the following throughput of at-least: • 779Mbps Threat prevention • 1.49Gbps NGFW • 1.9Gbps Intrusion Prevention • 3.2Gbps Firewall	
7	Must support at least 2million concurrent connections per second	
8	The hardware appliance must be new and does not have an End of Life (EOL) for the next five years upon delivery. Must submit certification or product data sheet.	
General Requirements:		
9	The solution must be an enterprise firewall that have a Unified Threat Management (UTM) and Intrusion Prevention capabilities.	
10	The solution must be able to comply the requirements, including throughput, connection rate and next generation security application enablement for all network deployments, from small office to data center in a single hardware appliance.	
11	The solution must be capable of supporting these next generation firewall security requirements on a unified platform: • Stateful Inspection Firewall • Intrusion Prevention System • User Identity Acquisition • Application Control and URL filtering • Anti – Bot and Anti – Virus • Threat Emulation (Sandboxing)	

	• Threat Extraction (scrubbing) • HTTPS Inspection • Identity Awareness • IPSec VPN • Security Policy Management • Monitoring and Logging • Logging and Status • Event Correlation and Reporting	
Next Generation Firewall (NGFW) Functionality		
12	The firewall solution must use Stateful Inspection based on granular analysis of communication and application state to track and control the network flow.	
13	Solution must support access control for at least 150 predefined /services/protocols	
14	Support an unlimited number of languages in UserCheck objects.	
15	Support Accelerated Policy Installation	
16	Support Concurrent Security Policy installation	
17	Support for Dynamic Policy	
18	Support for Domain objects, Updatable objects, Security Zones, Access Roles and Data Center objects.	
19	Support Hit count for NAT rules	
20	Must provide security rule hit count statistics to the management application.	
21	Must allow security rules to be enforced within time intervals to be configured with an expiry date/time.	
22	The communication between the management servers and the security gateways must be encrypted and authenticated with PKI Certificates.	
23	Solution must include a local user database to allow user authentication and authorization without the need for an external device	
IPsec VPN (Site to Site)		
24	Internal CA and External third-party CA must be supported	
25	Solution must support 3DES and AES-256 cryptographic for IKE Phase I and II IKEv2 plus "" and "Suite-B-GCM-256" for phase II	
26	Solution must support at least the following Diffie-Hellman Groups: Group 1 (768 bit), Group 2 (1024 bit), Group 5 (1536 bit), Group 14 (2048 bit), Group 19 and Group 20	
27	Solution must support data integrity with md5, sha1 SHA-256, SHA-384 and AES-XCBC	
28	Solution must include support for site-to-site VPN in the following topologies: • Full Mesh (all to all), • Star (remote offices to central site) • Hub and Spoke (remote site through central site to another remote site)	
29	Solution must support the VPN configuration with a GUI using drag and drop object to VPN communities	
30	Solution must support clientless SSL VPNs for remote access.	
31	Solution must support L2TP VPNs, including support for iPhone L2TP client	
32	Solution must allow the administrator to apply security rules to control the traffic inside the VPN	
33	Solution must include the ability to establish VPNs with gateways with dynamic public IPs	

34	Solution must include IP compression for client-to-site and site-to-site VPNs	
35	Solution must support VTI - VPN Tunnel Interface (with Route Based VPN, BGP and OSPF Dynamic Routing).	
36	Solution must support Link Selection & Service Based Link Selection	
37	Solution must support Back-to-back tunnels (hub and spokes)	
Advanced Threat Prevention		
38	The solution must provide the ability to Protect against zero-day & unknown malware attacks before static signature protections have been created. • Real-Time Prevention-unknown malware patient-0 in web browsing • Real-Time Prevention-unknown malware patient-0 in email	
38	Support zero-day phishing websites	
39	Support dynamic security components	
40	IoC feeds should support a significantly greater number of observables for URLs, Domains, IP addresses, and Hashes	
41	The solution should be part of a complete multi-layered threat prevention architecture (with IPS,AV,AB,URLF,APP FW)	
42	The solution should Eliminate threats and remove exploitable content, including active content and embedded objects	
43	The solution should be able to Reconstruct files with known safe elements	
44	The solution should Provide ability to convert reconstructed files to PDF format	
45	Support for Password-Protected Documents: Admins can now configure a default action for password-protected documents.	
46	Prevent multi-stage attacks	
47	Support MITRE ATT&CKTM Reporting	
48	Support for Archive Files - this engine release includes significant improvements in handling archive files	
49	The proposed security brand should have the lowest False Positive Detection Rate 0.13% by the third party institution. Please provide reference document to validate.	
50	The proposed brand should have the highest B2:D118 malware catch rate 99.7% using Prevention only methods by the third party institution. Please provide reference document to validate.	
Application Control and URL Filtering		
51	The proposed NGFW solution must provide application control for known applications.	
52	The proposed solution must have an advanced URL filtering and must be able to analyze, categorized, and blocking of malicious URLs in real time.	
53	The solution must be able to create filtering rules with multiple categories or single site being supported by multiple categories.	
54	The solution must have an easy to use, searchable interface for applications and URLs	
55	The solution must categorize applications and URLs. In addition, the solution should also support applications by Risk Factor	
56	The application control and URLF security policy must be able to be defined by user identities	
57	The application control and URLF database must have an automatic update service.	
58	The solution must have unified application control and URLF security rules	

59	The solution must provide a mechanism to limit application usage based on bandwidth consumption	
60	The solution must allow network exceptions based on defined network objects	
61	The solution must provide the option to modify the Blocking Notification and to redirect the user to a remediation page	
62	The solution must include a Black- and Whitelists mechanism to allow the administrator to deny or permit specific URLs regardless of the category	
62	The solution must have a configurable bypass mechanism	
64	The solution must provide an override mechanism on the categorization for the URL database	
65	The application control and URLF security policy must report on the rule hit count	
Advanced Intrusion Prevention System (IPS)		
66	IPS must be based on the following detection mechanisms: exploit signatures, protocol anomalies, application controls and behavior-based detection	
67	IPS and firewall module must be integrated on one platform.	
68	The administrator must be able to configure the inspection to protect internal hosts only	
69	IPS must have options to create profiles for either client or server-based protections, or a combination of both	
70	IPS must provide at least two pre-defined profiles/policies that can be used immediately	
71	IPS must have a software-based fail-open mechanism, configurable based on thresholds of security gateways CPU and memory usage	
72	IPS application must have a centralized event correlation and reporting mechanism	
73	The administrator must be able to automatically activate new protections, based on configurable parameters (performance impact, threat severity, confidence level, client protections, server protections)	
74	The administrator must be able to define network and host exclusions from IPS inspection	
75	Solution must protect from DNS Cache Poisoning, and prevents users from accessing blocked domain addresses	
76	IPS must have a mechanism to convert SNORT signatures	
Supplier's Eligibility Requirements		
77	The supplier must be at least five (5) Years of existence in the IT Industry. Information should be based on SEC (Security and Exchange Commission) incorporation information, that the vendor is at least five (5) years. The bidder must submit a notarize certification from them with reference to SEC documents.	
78	The supplier must be an authorized reseller or distributor of the brand being offered. Must submit certification from the distributor or principal.	
79	The supplier must have at least two (2) local Information Technology (IT) engineers to support the configurations and provide onsite support. Must submit the following: • Certificate of employment (must have at-least 3 years of work experience and have handled the proposed firewall products for at-least a year) • Resume or Curriculum Vitae • Trainings and Seminars (including with the proposed firewall solution)	

80	Three (3) years warranty on hardware and software. Warranty shall also cover any reconfiguration/integration after successful implementation with four-hour Hardware Replacement Service (RMA). (The warranty certificate will be submitted by the winning bidder)	
81	The Manufacturer or Distributor must have local sales and technical office in the Philippines for guaranteed support. Bidder must submit the Manufacturer's address, contact number, and contact person.	
82	The supplier must have a local helpdesk to provide 24x7 technical assistance. Must provide detailed escalation procedure and support including contact numbers and email addresses.	
83	The supplier must have a dedicated Project Manager (PM) to oversee the project. Must submit Certificate of Employment and Resume/Curriculum Vitae with at-least five years work experience on how to handle IT projects. Must submit the list of the Project handled, include the End-User/Client company name, Project Name and Project Duration (Start date and end-date)	
84	**The supplier must have at least Two (2) installed based Next Generation Firewall of the same brand or any equivalent NGFW being offered wherein one (1) is a Philippine commercial or universal bank. Must provide the client/bank name, contact person, address, telephone number and email). Landbank will sign the NDA for confidentiality if needed.**	
85	In the event that the Problem requires escalation to manufacturer, the supplier must have access and can escalate to manufacturer's Technical Center (TAC). Must provide detailed escalation to TAC.	
86	The Bidder must provide knowledge transfer training for at-least five (5) LBP IT personnel	
Other Requirements		
87	The Winning Bidder must comply with the requirements in relation to Third Party/Vendor Assessment conducted by the Bank internal audit and external audit such as Bangko Sentral ng Pilipinas (BSP), Commission on Audit (COA), etc.	
88	Must submit [e.g., Latest Financial Statement (FS), Business Continuity Plan (BCP) that are related to the Bank, and List of Updated Technical Support (include name, contact numbers and email address), etc]	
89	The vendor and/or supplier must notify the bank IT personnel of any related cyber security supply chain incidents such as, but not limited to compromise/breaches involving the vendor/supplier data, the product hardware or software, etc. It must be reported within a risk-informed time frame of 24 hours upon learning of the incident.	
90	The vendor and/or supplier must notify the bank IT personnel of any critical security vulnerability, firmware upgrade and performance patches and fixes that is needed to be applied.	
Delivery Terms and Conditions		
91	Delivery after receipt of NTP: 60 calendar days	
92	Installation will start 7 calendar days after delivery and will end 90 calendar days after.	
93	Delivery Site: Land Bank Head Office	
Delivery and Payment Terms		
94	The supplier must submit the following requirements for payment: • Sales invoice/Billing Statement/Statement of Account • Delivery Receipt with printed name and signature of LANDBANK employee who received the delivery and actual date of receipt of items.	

	Payment shall be through direct credit to the supplier's deposit account with LANDBANK. The supplier is required to maintain a deposit account with LANDBANK's Cash Department or any of its Branches.	
95	One-time Payment	

Prepared by:

JAY-R B. JADREN
ITO - LAN Team

Checked by:

ARCHIEVAL B. TOLENTINO
ITM - LAN Team

Approved by:

ENRIQUE L. SAZON JR.
VP - NOD

Revised D - 6

Technical Specifications

Specifications	Statement of Compliance **Bidders must state below either "Comply" or "Not Comply" against each of the individual parameters of each Specification preferably stating the corresponding performance parameter of the product offered.** Statements of "Comply" or "Not Comply" must be supported by evidence in a Bidders Bid and cross-referenced to that evidence. Evidence shall be in the form of manufacturer's un-amended sales literature, unconditional statements of specification and compliance issued by the manufacturer, samples, independent test data etc., as appropriate. A statement that is not supported by evidence or is subsequently found to be contradicted by the evidence presented will render the Bid under evaluation liable for rejection. A statement either in the Bidders statement of compliance or the supporting evidence that is found to be false either during Bid evaluation, post-qualification or the execution of the Contract may be regarded as fraudulent and render the Bidder or supplier liable for prosecution subject to the applicable laws and issuances.
Supply, Delivery and Installation of Small Network Firewalls with Three (3) Years Warranty and Support 1. **Minimum technical specifications and other requirements per attached Revised Terms of Reference (Annexes D-1 to D-6)** 2. **The documentary requirements enumerated in Revised Annexes D-4 and D-5 (Vendor Requirements) of the Terms of Reference shall be submitted in Eligibility and Technical Component to support the compliance of the Bid to the technical specifications and other requirements.** Non-submission of the above documents may result in the post-disqualification of the bidder.	**Please state here either "Comply" or "Not Comply"**

Conforme:

_____
Name of Bidder

_____
Signature over Printed Name of
Authorized Representative

_____
Position

Checklist of Bidding Documents for Procurement of Goods and Services

The documents for each component should be arranged as per this Checklist. Kindly provide guides or dividers with appropriate labels.

Eligibility and Technical Component (PDF File)

- ***The Eligibility and Technical Component shall contain documents sequentially arranged as follows:***

  - **Eligibility Documents – Class "A"**

    Legal Eligibility Documents

    1. Valid PhilGEPS Registration Certificate (Platinum Membership) (all pages)

    Technical Eligibility Documents

    2. Duly notarized Secretary's Certificate attesting that the signatory is the duly authorized representative of the prospective bidder, and granted full power and authority to do, execute and perform any and all acts necessary and/or to represent the prospective bidder in the bidding, if the prospective bidder is a corporation, partnership, cooperative, or joint venture; or Original Special Power of Attorney of all members of the joint venture giving full power and authority to its officer to sign the OSS and do acts to represent the Bidder. (sample form - Form No. 7).
    3. Statement of the prospective bidder of all its ongoing government and private contracts, including contracts awarded but not yet started, if any, whether similar or not similar in nature and complexity to the contract to be bid, within the last five (5) years from the date of submission and receipt of bids. The statement shall include all information required in the sample form (Form No. 3).
    4. Statement of the prospective bidder identifying its Single Largest Completed Contract (SLCC) similar to the contract to be bid within the relevant period as provided in the Bidding Documents. The statement shall include all information required in the sample form (Form No. 4).

Financial Eligibility Documents

5. The prospective bidder's audited financial statements, showing, among others, the prospective bidder's total and current assets and liabilities, stamped "received" by the BIR or its duly accredited and authorized institutions, for the preceding calendar year which should not be earlier than two (2) years from the date of bid submission.

6. The prospective bidder's computation for its Net Financial Contracting Capacity (NFCC) following the sample form (Form No. 5), or in the case of Procurement of Goods, a committed Line of Credit from a Universal or Commercial Bank in lieu of its NFCC computation.

- **Eligibility Documents – Class "B"**

7. Duly signed valid joint venture agreement (JVA), in case the joint venture is already in existence. In the absence of a JVA, duly notarized statements from all the potential joint venture partners stating that they will enter into and abide by the provisions of the JVA in the instance that the bid is successful shall be included in the bid. Failure to enter into a joint venture in the event of a contract award shall be ground for the forfeiture of the bid security. Each partner of the joint venture shall submit its legal eligibility documents. The submission of technical and financial eligibility documents by any of the joint venture partners constitutes compliance, provided, that the partner responsible to submit the NFCC shall likewise submit the statement of all its ongoing contracts and Audited Financial Statements.

8. For foreign bidders claiming by reason of their country's extension of reciprocal rights to Filipinos, Certification from the relevant government office of their country stating that Filipinos are allowed to participate in government procurement activities for the same item or product.

9. Certification from the DTI if the Bidder claims preference as a Domestic Bidder.

- **Technical Documents**

10. Bid Security (if in the form of a Surety Bond, submit also a certification issued by the Insurance Commission).
11. Section VI – Schedule of Requirements with signature of bidder's authorized representative.

12. **Section VII – Revised Specifications with response on compliance and signature of bidder's authorized representative.**
13. Duly notarized Omnibus Sworn Statement (OSS) (sample form - Form No.6).

Note: During the opening of the first bid envelopes (Eligibility and Technical Component), only the above documents will be checked by the BAC if they are all present using a non-discretionary "pass/fail" criterion to determine each bidder's compliance with the documents required to be submitted for eligibility and the technical requirements.

- **Other Documents to Support Compliance with Technical Specifications [must be submitted inside the first bid envelope (Eligibility and Technical Component)]**

14. **Duly filled-out Revised Terms of Reference signed in all pages by the authorized representative/s of the bidder.**
15. Notarized Certification with reference to Registration from the Securities and Exchange Commission as proof that bidder has at least five (5) years existence in the IT industry.
16. Manufacturer's authorization (sample form - Form No. 9) or its equivalent document, confirming that the bidder is authorized to provide the brand being offered and consumables supplied by the manufacturer, including any warranty obligations and after sales support as may be required.
17. Certificate of Employment, Resume/Curriculum Vitae and Certificate of Trainings and Seminars attended (including seminar on proposed firewall solution) of at least two (2) local Information Technology engineers with at least three (3) years work experience and have handled firewall products for at least one (1) year.
18. List of local sales and technical office in the Philippines with contact person, address, contact number and email address.
19. Certificate of Employment, Resume/Curriculum Vitae and List of Projects Handled (with client/company name, project name and project duration) of the dedicated Project Manager with at least five (5) years work experience in handling IT projects.

20. **List of at least two (2) installed based in the Philippines, with one (1) Commercial or Universal Philippine Bank, of the same product and brand or any equivalent Next Generation Firewall being offered with client name, contact person, complete address, contact number and email address.**

21. Detailed Escalation Procedure and Support including contact numbers and email addresses.

- **Post-Qualification Documents/Requirements – [The bidder may submit the following documents/requirements within five (5) calendar days after receipt of Notice of Post-Qualification]:**

22. Business Tax Returns per Revenue Regulations 3-2005 (BIR No.2550 Q) VAT or Percentage Tax Returns for the last two (2) quarters filed manually or through EFPS.
23. Latest Income Tax Return filed manually or through EFPS.
24. Original copy of Bid Security (if in the form of a Surety Bond, submit also a certification issued by the Insurance Commission).
25. Original copy of duly notarized Omnibus Sworn Statement (OSS) (sample form - Form No.6).
26. Duly notarized Secretary's Certificate designating the authorized signatory in the Contract Agreement if the same is other than the bidder's authorized signatory in the bidding (sample form – Form No. 7).

Financial Component (PDF File)

- ***The Financial Component shall contain documents sequentially arranged as follows:***

1. Duly filled out Bid Form signed by the Bidder's authorized representative (sample form - Form No.1).
2. Duly filled out Schedule of Prices signed by the Bidder's authorized representative (sample form - Form No.2).
3. Duly filled out Bill of Quantities Form signed by the bidder's authorized representative (Annex E)

Note: The forms attached to the Bidding Documents may be reproduced or reformatted provided the information required in the original forms and other requirements like signatures, if applicable, are complied with in the submittal.

RESPONSES TO BIDDER'S QUERIES AND/OR SUGGESTIONS

RESPONSES TO BIDDER'S QUERIES AND/OR SUGGESTIONS DATE	NOVEMBER 15, 2023
PROJECT IDENTIFICATION NO.	LBP-ICTBAC-ITB-GS-20230926-02
PROJECT NAME	Supply, Delivery and Installation of Small Network Firewalls with Three (3) Years Warranty and Support
PROPONENT UNIT/TECHNICAL WORKING GROUP	Network Operations Department

ITEM NO.	PORTION OF BIDDING DOCUMENTS	QUERIES AND /OR SUGGESTIONS	LANDBANK'S RESPONSES
84	The supplier must have at-least Two (2) installed based Next Generation Firewall product of the SAME BRAND being offered wherein one (1) is a Philippine commercial or universal bank. Must provide the client/bank name, contact person, address, telephone number and email). Landbank will sign the NDA for confidentiality if needed.	**MDI Inquiry:** May we request to relax the word "SAME BRAND" with Same or any Equivalent NGFW Brand deployed in HA mode instead?	**Yes, we're amenable.** **For TOR Revision:** The supplier must have at least Two (2) installed based Next Generation Firewall of the same brand or any equivalent NGFW being offered wherein one (1) is a Philippine commercial or universal bank. Must provide the client/bank name, contact person, address, telephone number and email). Landbank will sign the NDA for confidentiality if needed.

Prepared By:

Jay-R G. Jadren
ITO, NOD

Reviewed By:

Archieval B. Tolentino
ITM, NOD

RESPONSES TO BIDDER'S QUERIES AND/OR SUGGESTIONS

RESPONSES TO BIDDER'S QUERIES AND/OR SUGGESTIONS DATE	NOVEMBER 15, 2023
PROJECT IDENTIFICATION NO.	LBP-ICTBAC-ITB-GS-20230926-02
PROJECT NAME	Supply, Delivery and Installation of Small Network Firewalls with Three (3) Years Warranty and Support
PROPONENT UNIT/TECHNICAL WORKING GROUP	Network Operations Department
Bidders	**One Commerce (Int'l.) Corporation**

ITEM NO.	PORTION OF BIDDING DOCUMENTS	QUERIES AND /OR SUGGESTIONS	LANDBANK'S RESPONSES
91	Delivery after receipt of NTP: 60 calendar days	a. Is the timeline for delivery and installation separate?	Yes.
92	Installation will start 7 calendar days after delivery and will end 90 calendar days after.	b. Will the 60 calendar days be deducted within the 90 calendar days after delivery?	No, the 90 calendar days will start upon the initial installation.
		Request a fourteen (14)-day extension	No, we have a timeline for the project.

Prepared By:

Jay-R C. Jadrien
ITO, NOD

Reviewed By:

Archieval B. Tolentino
ITM, NOD

H-2