Republic of the Philippines
Department of Finance
INSURANCE COMMISSION
1071 United Nations Avenue, Manila

BAGONG PILIPINAS

BIDS AND AWARDS COMMITTEE
SUPPLEMENTAL BID BULLETIN NO. 1

Maintenance Service Agreement and Licenses for the Existing Next-Generation Firewall Appliance
(Project Reference No. 2025 – 04 – 233)

This Supplemental Bid Bulletin No. 1, dated 09 June 2025, is being issued to clarify, modify, or amend items in the Bidding Documents.

The following Items in the Bidding Documents for the ***Maintenance Service Agreement and Licenses for the Existing Next-Generation Firewall Appliance,*** dated 24 May 2025, are hereby revised/amended:

1. Amendment of **Section VII. Technical Specifications**, **Item No. 4. Specifications:**

   FROM :

   The winning bidder shall provide licenses and support to the Palo Alto Next Generation Firewall Appliance with the following details:

   Model: Palo Alto 3410
   Serial Number: 024101006551
   Features:

   - Premium Partner
   - Threat Prevention
   - Advanced Threat Prevention
   - DNS Security
   - Advanced URL Filtering
   - Advanced Wildfire License

   Management, Reporting, Logging, and Policy Checking Features

   - Must be manageable from a web-based Graphical User Interface (GUI) and Command-Line Interface (CLI) without the need for external servers or appliances, at the same time with a capability to be managed centrally.
   - Must be able to delegate appropriate role-based administrative access controls to administrators.
   - Must have a highly customizable user interface for applications, users, content, and security threats.

- 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 for any additional software subscription, licenses, or hardware components.
- The firewall Layer 7 functionality must have application dependency checks and warnings that notify the administrator when dependent applications must be added to a policy rule in order for a given application/s to operate properly.

Premium Support Features

- The firewall must have direct access to product experts: Interact with a support engineer trained to quickly understand and resolve your unique challenges.
- The firewall must have 24x7 support for issues of all severities, with Platinum senior engineers available around the clock to assist.
- The firewall must have a feature-rich platform that provides access to product documentation, problem resolution databases, peer-to-peer interaction, and support case management.
- The firewall must have an assisted security investigation.
- The firewall must have an advanced log & IOC analysis and next steps recommendations.
- The firewall must have a pre-scheduled event support.
- The firewall must have on-site assistance for critical issues (after remote troubleshooting).
- The firewall must have a failure analysis (HW).

Threat Prevention Features

- Must have natively integrated IPS, anti-spyware, anti-malware, and Command-and-Control (C2) prevention capabilities.
- Must be able to perform stream-based antivirus inspection and not proxy-based or store-and-forward traffic inspection.
- Must be able to block known network and application-layer vulnerability exploits.
- Must have the capability to act as a multi-factor authentication gateway for various enterprise applications to prevent credential theft and abuse that may lead to unauthorized access, modification, and stealing of sensitive data.
- Must have the ability to apply predictive analytics to interrupt bad actors that use DNS for C&C or data theft.
- Shall have an effective detection of malware and exploits that compliment dynamic analysis, as well as provide instant identification of malware variants.
- Shall be able to send the evasive threat to a real hardware environment for detonation, entirely removing an adversary’s ability to deploy anti-VM analysis techniques.
- Can be able to execute suspicious content in Windows XP, Windows 7, Windows 10, Windows 11, Android, and macOS operating systems.
- Shall be able to perform analysis of all network activity produced by the suspicious file, including back door creation, downloading of next-stage malware, visiting low-reputation domains, and network reconnaissance.

- Can monitor techniques used by advanced malware that are designed to avoid VM-based analysis, such as debugger detection, hypervisor detection, code injection into trusted processes, and disabling of host-based security features.
- Shall have full visibility into all network traffic, including stealthy attempts to evade detection, such as the use of non-standard ports or SSL encryption.

URL Filtering Features

- Must have natively integrated URL filtering capabilities.
- Must have a local database of URL categories for faster response and not primarily dependent on cloud database inquiries. The license must be perpetual and must still function even if expired.
- Must have an automated cloud-based dynamic URL categorization for classifying unknown web sites.
- Must have a specific category for Malware, Phishing, Command-and-Control, Proxy Avoidance, and Anonymizers, among other usual web categories.
- URL Database stopping known threats and cloud-delivered web security engine powered by machine.
- The ability to have granular controls and policy settings that enable administrators to automate security actions based on users, risk ratings, and content categories.
- Beyond webpage crawling to analyze live web content, disrupting attackers, and identifying the true nature of malicious sites hiding behind evasive techniques.
- Utilize URL categories to set off additional security procedures automatically, such as selective TLS/SSL decryption for suspicious sites.
- Credential theft protection.
- Selective SSL Decryption.

Bidders Certifications and Qualifications

- The bidder must provide a Certificate as an Authorized Distributor/ Partner/Dealer/Reseller from the Manufacturer/Principal of the brand being offered.
- Bidder must be a certified partner of the proposed brand for at least five (5) years.
- To ensure comprehensive support capabilities for the proposed NGFW solution, the bidder must be of the highest/tier 1/platinum partnership with the solution manufacturer. This partnership level would ensure that the partner of IC would have in-depth technical resources, training, and support programs directly from the manufacturer.
- The bidder must have the following technical support and experience:
    - Three (3) Palo Alto Certified Network Security Engineers with at least Three (3) years of experience working in a similar field of engagement.
    - Five (5) Technical Support Engineers that can support Palo Alto Appliance of IC with at least Three (3) years of experience working in a similar field of engagement.

    - Two (2) Installed Base of Palo Alto Firewall.
- Bidder must be duly established in the Philippines with at least twenty (20) years of experience in the supply, delivery, and installation of ICT products and solutions.
    - Attach Company Profile
    - Vicinity map/location of the business
- Bidder must have a 24 x 7 helpdesk system via phone and email support. The helpdesk system must automatically track, monitor, and escalate open cases until the issue is declared resolved and closed. The vendor should be ready for a site visit and show how their current helpdesk system works.

TO :

Model: Palo Alto 3410
Serial Number: 024101006551
Features:

- ***<u>Premium Partner / Support</u>***
- Threat Prevention
- Advanced Threat Prevention
- ***<u>Advanced DNS Security</u>***
- Advanced URL Filtering
- Advanced Wildfire License

Management, Reporting, Logging, and Policy Checking Features

- Must be manageable from a web-based Graphical User Interface (GUI) and Command-Line Interface (CLI) without the need for external servers or appliances, at the same time with a capability to be managed centrally.
- Must be able to delegate appropriate role-based administrative access controls to administrators.
- Must have a highly customizable user interface for applications, users, content, and security threats.
- 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 for any additional software subscription, licenses, or hardware components.
- The firewall Layer 7 functionality must have application dependency checks and warnings that notify the administrator when dependent applications must be added to a policy rule in order for a given application/s to operate properly.

Premium Support Features

- The firewall must have direct access to product experts: Interact with a support engineer trained to quickly understand and resolve your unique challenges.
- ***<u>The firewall must have 24x7 support for issues of all severities, with support engineers available at all times to assist.</u>***

- The firewall must have a feature-rich platform that provides access to product documentation, problem resolution databases, peer-to-peer interaction, and support case management.
- The firewall must have an assisted security investigation.
- The firewall must have an advanced log & IOC analysis and next steps recommendations.
- ***<u>The firewall must have on-site assistance for critical issues (after remote troubleshooting) by the winning bidder.</u>***

Threat Prevention Features

- Must have natively integrated IPS, anti-spyware, anti-malware, and Command-and-Control (C2) prevention capabilities.
- Must be able to perform stream-based antivirus inspection and not proxy-based or store-and-forward traffic inspection.
- Must be able to block known network and application-layer vulnerability exploits.
- Must have the capability to act as a multi-factor authentication gateway for various enterprise applications to prevent credential theft and abuse that may lead to unauthorized access, modification, and stealing of sensitive data.
- Must have the ability to apply predictive analytics to interrupt bad actors that use DNS for C&C or data theft.
- Shall have an effective detection of malware and exploits that compliment dynamic analysis, as well as provide instant identification of malware variants.
- Shall be able to send the evasive threat to a real hardware environment for detonation, entirely removing an adversary's ability to deploy anti-VM analysis techniques.
- ***<u>Can be able to execute suspicious content in Windows XP, Windows 7, Windows 10, Android, and macOS operating systems.</u>***
- Shall be able to perform analysis of all network activity produced by the suspicious file, including back door creation, downloading of next-stage malware, visiting low-reputation domains, and network reconnaissance.
- Can monitor techniques used by advanced malware that are designed to avoid VM-based analysis, such as debugger detection, hypervisor detection, code injection into trusted processes, and disabling of host-based security features.
- Shall have full visibility into all network traffic, including stealthy attempts to evade detection, such as the use of non-standard ports or SSL encryption.

URL Filtering Features

- Must have natively integrated URL filtering capabilities.
- ***<u>Must have a local database of URL categories for faster response and not primarily dependent on cloud database inquiries.</u>***
- Must have an automated cloud-based dynamic URL categorization for classifying unknown web sites.
- Must have a specific category for Malware, Phishing, Command-and-Control, Proxy Avoidance, and Anonymizers, among other usual web categories.

- URL Database stopping known threats and cloud-delivered web security engine powered by machine.
- The ability to have granular controls and policy settings that enable administrators to automate security actions based on users, risk ratings, and content categories.
- Beyond webpage crawling to analyze live web content, disrupting attackers, and identifying the true nature of malicious sites hiding behind evasive techniques.
- Utilize URL categories to set off additional security procedures automatically, such as selective TLS/SSL decryption for suspicious sites.
- Credential theft protection.
- Selective SSL Decryption.

Bidders Certifications and Qualifications

- The bidder must provide a Certificate as an Authorized Distributor/ Partner/Dealer/Reseller from the Manufacturer/Principal of the brand being offered.
- Bidder must be a certified partner of the proposed brand for at least five (5) years.
- To ensure comprehensive support capabilities for the proposed NGFW solution, the bidder must be of the highest/tier 1/platinum partnership with the solution manufacturer. This partnership level would ensure that the partner of IC would have in-depth technical resources, training, and support programs directly from the manufacturer.
- The bidder must have the following technical support and experience:
    - ***Two (2) Palo Alto Certified Network Security Engineers*** with at least Three (3) years of experience working in a similar field of engagement.
    - Five (5) Technical Support Engineers that can support Palo Alto Appliance of IC with at least Three (3) years of experience working in a similar field of engagement.
    - Two (2) Installed Base of Palo Alto Firewall.
- Bidder must be duly established in the Philippines with at least twenty (20) years of experience in the supply, delivery, and installation of ICT products and solutions.
    - Attach Company Profile
    - Vicinity map/location of the business
- Bidder must have a 24 x 7 helpdesk system via phone and email support. The helpdesk system must automatically track, monitor, and escalate open cases until the issue is declared resolved and closed. The vendor should be ready for a site visit and show how their current helpdesk system works.

This Supplemental Bid Bulletin No. 1 shall form part of the Bid Documents. Any provisions in the Bid Documents inconsistent herewith is hereby amended, modified and superseded accordingly.

For the information and guidance of all concerned.

Issued this **09 June 2025** in the City of Manila.

ARTURO S. TRINIDAD II
Chairperson
Bids and Awards Committee

Supplemental Bid Bulletin No. 1 for the ***Maintenance Service Agreement and Licenses for the Existing Next-Generation Firewall Appliance*** dated 09 June 2025, consisting of eight (8) pages.

Received by: ____

Name of the Bidder/Company: ____

Name of Authorized Representative/s: ___________________________________

Signature/s: ____

Date: ____________________