REPUBLIC OF THE PHILIPPINES

DEPARTMENT OF BUDGET AND MANAGEMENT

GENERAL SOLANO STREET, SAN MIGUEL, MANILA

SUPPLEMENTAL/BID BULLETIN (SBB) NO. 1

This SBB No. 1 dated October 29, 2021 for **Project No. DBM-2022-04, "Fortinet Equipment Refresh,"** is issued pursuant to Section 22.5 of the 2016 Revised Implementing Rules and Regulations of Republic Act No. 9184, to clarify, modify or amend items in the Bidding Documents. Accordingly, this shall form an integral part of the Bidding Documents.

PARTICULARS	AMENDMENTS
Section VII. Technical Specifications **Annex "A" (Detailed Technical Specifications)** xxx **4.0 Scope of Work** xxx 4.1.4.7 Should have the following interfaces, such as but not limited to the following: 4.1.4.7.1 2x GbE RJ 45 4.1.4.7.2 2x SFP	**Section VII. Technical Specifications** **Annex "A" (Detailed Technical Specifications)** xxx **4.0 Scope of Work** xxx 4.1.4.7 Should have ~~the following interfaces, but not limited to:~~ ~~4.1.4.7.1 2x GbE RJ 45~~ ~~4.1.4.7.2 2x SFP~~ **4X GBE RJ45 INTERFACE**
	Attached is Annex "A" (Detailed Technical Specifications) (Revised) which should be used as part of the Bidding Documents to be submitted by the bidders.

Other matters:

- The "No Contact Rule" shall be strictly observed. Bidders are not allowed to call or talk to any member of the Bids and Awards Committee, Technical Working Group or Secretariat effective November 5, 2021 right after the opening of bids.

- For guidance and information of all concerned.

Digitally signed by Janet B. Abuel

JANET B. ABUEL
Undersecretary
Chairperson, DBM-BAC

Annex A

Detailed Technical Specifications
(Revised)

1.0 PROJECT TITLE

Fortinet Equipment Refresh

2.0 OBJECTIVE

To replace the obsolete[1] Fortinet Equipment to ensure the connectivity and security of the DBM Information and Communication Technology (ICT) Infrastructure and Information Systems.

This project covers equipment that should be compatible and interoperable with the existing equipment in the DBM Data Center. Hence, reference to brand names is authorized under Section 18 of the 2016 Revised IRR of RA 9184 which provides that, "[r]eference to brand names shall not be allowed **except for items or parts that are compatible with the existing fleet or equipment of the same make and brand, and to maintain the performance, functionality and useful life of the equipment**". (emphasis supplied)

3.0 IMPLEMENTATION PERIOD

The delivery, installation, configuration, testing, and commissioning of Fortinet Equipment shall be within ninety (90) calendar days from receipt of the Notice to Proceed (NTP).

4.0 SCOPE OF WORK

4.1 The Contractor shall deliver, install, configure, test, commission, and make operational the following Fortinet Equipment:

4.1.1 Two (2) units of Fortinet FortiGate 1101E[2] with the following minimum specifications:

4.1.1.1 Identifies thousands of applications inside network traffic for deep inspection and granular policy enforcement.
4.1.1.2 Protects against malware, exploits, and malicious websites in both encrypted and non-encrypted traffic.
4.1.1.3 Prevents and detects against known attacks using continuous threat intelligence from AI-powered FortiGuard Labs security services.
4.1.1.4 Proactively blocks unknown sophisticated attacks in real-time with the Fortinet Security Fabric integrated AI-powered FortiSandbox.

[1] end of useful life and end of support

[2] To replace FortiGate 1000C units acquired year 2014 and 2016

4.1.1.5 Provides protection for SSL encrypted traffic including TLS 1.3 deep inspection.
4.1.1.6 Application-aware routing with in-built SD-WAN capabilities to achieve consistent application performance and the best user experience.
4.1.1.7 Built-in advanced routing capabilities to deliver high performance with encrypted IPSEC tunnels at scale.
4.1.1.8 Automatically builds Network Topology visualizations that discover IoT devices and provide complete visibility.
4.1.1.9 Should have the following interfaces per unit, but not limited to:

4.1.1.9.1 Console Port
4.1.1.9.2 2x USB Ports
4.1.1.9.3 2x GE RJ45 Management / HA Ports
4.1.1.9.4 16x GE RJ45 Ports
4.1.1.9.5 8x GE SFP Slots
4.1.1.9.6 4x 10 GE SFP+ Slots
4.1.1.9.7 4 x 25 GE SFP28/ 10
4.1.1.9.8 2x 40 GE QSFP+ Slots

4.1.1.10 2x 480 GB Solid State Drive onboard storage
4.1.1.11 Redundant hot-swappable power supply
4.1.1.12 Should have the following system performance and capacity, but not limited to:

4.1.1.12.1 12.5 Gbps IPS Throughput
4.1.1.12.2 9.8 Gbps NGFW Throughput
4.1.1.12.3 7.1 Gbps Threat Protection Throughput
4.1.1.12.4 8 Million Concurrent Sessions (TCP)
4.1.1.12.5 500,00 New Sessions/Second (TCP)
4.1.1.12.6 100,000 Firewall Policies
4.1.1.12.7 20,000 Gateway-to-Gateway IPsec VPN Tunnels
4.1.1.12.8 100,000 Client-to-Gateway IPsec VPN Tunnels
4.1.1.12.9 8.4 Gbps SSL-VPN Throughput
4.1.1.12.10 10,000 Maximum concurrent SSL-VPN Users
4.1.1.12.11 10 Gbps SSL Inspection Throughput (HTTPS)

4.1.1.13 High Availability Configurations

4.1.1.13.1 Active-Active
4.1.1.13.2 Active-Passive
4.1.1.13.3 Clustering

4.1.1.14 Should be bundled with Enterprise Protection Software Licenses

4.1.2 Eighteen (18) units of Fortinet Fortigate 101F[3] with the following minimum specifications:

[3] To replace Fortigate-90D units acquired year 2014 (including additional service units)

4.1.2.1 Identifies thousands of applications inside network traffic for deep inspection and granular policy enforcement.
4.1.2.2 Protects against malware, exploits, and malicious websites in both encrypted and non-encrypted traffic.
4.1.2.3 Prevents and detects against known attacks using continuous threat intelligence from AI-powered FortiGuard Labs security services.
4.1.2.4 Proactively blocks unknown sophisticated attacks in real-time with the Fortinet Security Fabric integrated AI-powered FortiSandbox.
4.1.2.5 Provides protection for SSL encrypted traffic including TLS 1.3 deep inspection.
4.1.2.6 Application-aware routing with in-built SD-WAN capabilities to achieve consistent application performance and the best user experience.
4.1.2.7 Built-in advanced routing capabilities to deliver high performance with encrypted IPSEC tunnels at scale.
4.1.2.8 Should have the following interfaces per unit, but not limited to:

4.1.2.8.1 Console Port
4.1.2.8.2 USB Port
4.1.2.8.3 2x GE RJ45 Management / DMZPorts
4.1.2.8.4 2x GE RJ45 WAN Ports
4.1.2.8.5 2x GE RJ45 HA Ports
4.1.2.8.6 12x GE RJ45 Ports
4.1.2.8.7 2x 10 GE SFP+FortLink Slots
4.1.2.8.8 4x GE SFP Slots
4.1.2.8.9 4x GE RJ45/SFP Shared Media Pairs

4.1.2.9 1x 480 GB Solid State Drive internal storage
4.1.2.10 Should have the following system performance and capacity, but not limited to:

4.1.2.10.1 2.6 Gbps IPS Throughput
4.1.2.10.2 1.6 Gbps NGFW Throughput
4.1.2.10.3 1 Gbps Threat Protection Throughput
4.1.2.10.4 1.5 Million Concurrent Sessions (TCP)
4.1.2.10.5 56,000 New Sessions/Second (TCP)
4.1.2.10.6 10,000 Firewall Policies
4.1.2.10.7 2,500 Gateway-to-Gateway IPsec VPN Tunnels
4.1.2.10.8 16,000 Client-to-Gateway IPsec VPN Tunnels
4.1.2.10.9 750 Mbps SSL-VPN Throughput
4.1.2.10.10 500 Maximum concurrent SSL-VPN Users
4.1.2.10.11 1 Gbps SSL Inspection Throughput (HTTPS)

4.1.2.11 Should be bundled with Enterprise Protection Software Licenses.

4.1.3 One (1) unit of Fortinet FortiManager 300F[4] with the following minimum specifications:

[4] To replace FortiManager-300D unit acquired year 2014

4.1.3.1 Single console management, manage all Fortinet products, including firewalls, FortiAnalyzers, switches, wireless infrastructure, and Endpoints Centralized policy and device management.
4.1.3.2 Centrally manage up to 100 firewall devices and policies such as firewalls, switches, and access points.
4.1.3.3 Automate workflows and configurations for Fortinet firewalls, switches, and wireless infrastructure.
4.1.3.4 Provision and monitor Secure SD-WAN from one console across your network, branch offices, or campuses.
4.1.3.5 Multi-tenancy and administrative domains (ADOMs), Separate customer data and manage domains leveraging ADOMs to be compliant and operationally effective.
4.1.3.6 Reduces complexity and costs by leveraging automated REST API, scripts, connectors, and automation stitches.
4.1.3.7 Enterprise-grade availability and integration, Automated backups up to 4 nodes with streamlined software and security updates for all managed devices.
4.1.3.8 Should have the following interfaces, but not limited to:
4.1.3.8.1 RJ 45 Console Port
4.1.3.8.2 4x GbE RJ 45
4.1.3.8.3 2x SFP
4.1.3.9 (4x 4 TB) 16TB internal storage, capable to support RAID 0/1/5/10
4.1.3.10 Should have the following system performance and capacity, but not limited to:
4.1.3.10.1 Maximum of 100 Devices/VDOMs
4.1.3.10.2 50 Sustained Log Rates, 2GB per day
4.1.3.11 Redundant Hot Swappable Power Supplies
4.1.3.12 Supports Removable Hard Drives

4.1.4 One (1) unit of Fortinet FortiAnalyzer 300G[5] with the following minimum specifications:

4.1.4.1 End-to-end visibility, Event correlation, threat detection, and Indicator of Compromise (IOC) service reduce time-to-detect and identity threats.
4.1.4.2 Fortinet Security Fabric integration, Correlates with logs from FortiClient, FortiSandbox, FortiWeb, and FortiMail for deeper visibility and critical network insights.
4.1.4.3 Enterprise-grade high availability, Automatically back-up FortiAnalyzer DB's (up to 4 node clusters) that can be geographically dispersed for disaster recovery.
4.1.4.4 Security automation, Reduce complexity, and leverage automation via REST API, scripts, connectors, and automation stitches to expedite security response.
4.1.4.5 Multi-tenancy and administrative domains (ADOMs), Separate customer data and manage domains leveraging, ADOMs to be compliant and operationally effective.

[5] To replace FortiAnalyzer-300D unit acquired year 2014

4.1.4.6 Flexible deployment options & archival storage, Supports the deployment of an appliance, VM, hosted, or cloud. Use Azure or Google to archive logs as secondary storage.
4.1.4.7 Should have 4x GbE RJ45 interface
4.1.4.8 (2x 4 TB) 8TB internal storage, capable to support RAID 0/1
4.1.4.9 Should have the following system performance and capacity, but not limited to:

4.1.4.9.1 100 GB per day of logs
4.1.4.9.2 2,000 log/sec Analytic Sustained Rate
4.1.4.9.3 3,000 log/sec Collector Sustained Rate
4.1.4.9.4 180 maximum Devices/VDOMs
4.1.4.9.5 28 maximum number of days analytics

4.1.4.10 Bundled with Indicator of Compromise Licenses/Services.

4.1.5 Transceiver Module

4.1.5.1 Twenty-six (26) units of FN-TRAN-SFP+SR (10 SFP+), as follows:

Quantity	Devices
4 units	FW1 – Fortinet Fortigate 1101E
4 units	FW2 – Fortinet Fortigate 1101E
18 units	Regional Fortinet 101F

4.1.5.2 Seventy (70) units of FN-TRAN-SX (1G SFP), as follows:

Quantity	Devices
6 units	FW1 – Fortinet Fortigate 1101E
6 units	FW2 – Fortinet Fortigate 1101E
54 units	Regional Fortinet 101F
2 units	Fortinet FortiManager 300F
2 units	Fortinet FortiAnalyzer 300G

4.1.5.3 Four (4) units of FG-TRAN-QSFP+SR, as follows:

Quantity	Devices
2 units	FW1 – Fortinet Fortigate 1101E
2 units	FW2 – Fortinet Fortigate 1101E

4.1.6 Migration of configuration and policies from existing devices (FortiGate 1000C, FortiGate 90D, FortiManager 300D, and FortiAnalyzer 300D) to the new respective devices.

4.1.7 Deployment of FortiGate 101F Firewall to the following DBM Regional Offices:
4.1.7.1 Region IV-A
4.1.7.2 National Capital Region

4.1.8 Configuration of High Availability for the FortiGate 1101E (Active-Active /Active-Passive)

4.2 The contractor shall conduct a pre-implementation meeting with DBM representatives so that all the necessary preparations, ideal set-up, contractor's familiarization of the computing environment, and other implementation matters are discussed and finalized.

4.3 The contractor shall provide a work plan of activities for the duration of the project and a Deployment and/or Solution Architecture within a week from the pre-implementation meeting with DBM representatives. Said work-plan shall be validated and subject to the approval of the Director of the Information and Communications Technology Systems Service (ICTSS).

4.4 The contractor must have the following Certified Professionals, with each certification represented by a different individual who will handle DBM requests and activities:

4.4.1 Fortinet Certified Network Security Expert (NSE) 5
4.4.2 Fortinet Certified Network Security Expert (NSE) 7
4.4.3 CISCO Certified Network Professional Enterprise

The corresponding certificates shall be submitted during post-qualification.

4.5 Maintenance and Technical Support Services

4.5.1 The CONTRACTOR must be able to provide a 24/7 3-tier support
4.5.1.1 Local reseller as the first-level support
4.5.1.2 Distributor as the second-level support
4.5.1.3 Principal as the third-level of support

4.5.2 During the warranty period, technical support shall be available twenty-four (24) hours a day, seven (7) days a week. Technical support may be delivered in the form of a telephone call, electronic mail, and/or on-site support as requested by the DBM.

Problems on software and hardware components, reported during the implementation period, shall be resolved to the satisfaction of the DBM within four (4) hours from receipt of the report.

4.6 During the warranty period**,** defective parts/accessories of the subject ICT equipment shall be replaced, at no additional cost to the DBM, with the same or better brand, model features, quality, and functionalities if the same is not repaired within the allowable resolution time of four (4) working hours.

4.7 During the warranty period, components (e.g., firmware upgrade, software update, patches, etc.) of the Fortinet equipment shall be kept up to date.

4.8 During the warranty period, conduct regular Fortinet Equipment preventive maintenance as required by the ICTSS. The results of such shall be documented in a report (e.g. status report, health check, performance, updates, recommendations, etc.) submitted within three (3) calendar days from the conduct of the activity.

4.9 The contractor shall resolve all reported issues encountered/unresolved under section 4.5.2 even the warranty ends.

4.10 The contractor shall provide Technical Training that can be a classroom type or online training based on the following schedule:

Technical Training	Schedule	No. of Participants	Duration
NSE 4 FortiGate Infra	Within thirty (30) calendar days from receipt of the NTP	Four (4) participants	Minimum of two (2) working days
NSE5 FortiManager	Within sixty (60) calendar days from receipt of the NTP	Four (4) participants	Minimum of two (2) working days
NSE5 FortiAnalyzer	Within ninety (90) calendar days from receipt of the NTP	Four (4) participants	Minimum of one (1) working day

The contractor shall issue individual training certificates and training materials for each of the participants.

4.11 The contractor shall provide as-built documentation of the Fortinet Equipment set-up/ diagram in both hard and soft copies including information in the deployment, system resource/overhead requirements of the software/IT equipment employed in the project as well as procedures for installation, uninstallation, configuration, integration, usage, backup and restoration within ninety (90) calendar days from receipt of the NTP.

5.0 SERVICE LEVEL AGREEMENT

5.1 DBM shall maintain a Service Level Agreement (SLA) with the contractor, with provisions for liquidated damages as indicated below for their non-compliance which shall be charged against any money due or which may become due to the contractor, or collected from any securities or warranties posted by the contractor.

Component	Description	Liquidated Damages
Delivery, Installation, Configuration, Testing, and Commissioning	The CONTRACTOR shall deliver, install, configure, test, and commission the Fortinet Equipment within ninety (90) calendar days from receipt of the NTP.	1/10th of 1% of the contract price for the undelivered portion shall be imposed per day of delay.

6.0 WARRANTIES OF THE CONTRACTOR

For the procurement of the project, the warranties shall include the following:

6.1 The contractor warrants that it shall conform strictly to the terms and conditions of this Detailed Technical Specifications.

6.2 The contractor warrants that the technical staff assigned are qualified to provide the deliverables required to the satisfaction of the DBM.

6.3 The contractor shall secure, maintain at its own expense all registration, licenses, or permits required by National or Local Laws and shall comply with the rules, regulations, and directives of Regulatory Authorities and Commissions. The contractor undertakes to pay all fees or charges payable to any instrumentality of government or any other duly constituted authorities relating to the use or operation of the installation.

6.4 The contractor's technical staff assigned to support DBM shall take all necessary precautions for the safety of all persons and properties at or near their area of work and shall comply with all the standard and established safety regulations, rules and practices.

6.5 The contractor's technical staff assigned to support DBM shall coordinate with the ICTSS in the implementation of this project.

6.6 The contractor shall be liable for loss, damage, or injury caused directly or indirectly by the fault or negligence of its technical staff assigned. It shall assume full responsibility thereof and the DBM shall be fully released from any liability arising therefrom.

6.7 The contractor shall neither assign, transfer, pledge, nor subcontract any part or interest to the contract being bidded out.

6.8 The contractor shall identify the certified technical support personnel that will be given authority to access and operate the specified equipment. The DBM shall be informed within five (5) calendar days, through a formal notice, of any change or replacement of technical staff assigned.

6.9 The contractor shall provide a two (2)-year comprehensive warranty which shall include technical support, provision of the service unit, parts replacement for the hardware/appliance, and preventive maintenance.

7.0 CONFIDENTIALITY OF DATA

7.1 All technical staff assigned by the contractor shall be required to sign a Non-Disclosure Agreement (NDA).

7.2 The DBM Enterprise Network System, its component, parts and all products, products samples and specifications, data, ideas, technology, and technical/non-technical materials, all or any which may be derived from any of the foregoing are strictly confidential.

7.3 The contractor agrees to hold all the foregoing information in strict confidence. The contractor further agrees not to reproduce or disclose any confidential information to third parties without the prior written approval of the DBM.

8.0 TERMS OF PAYMENT

One-time payment shall be made, subject to the submission of the following documentary requirements, and in accordance with budgeting, accounting, and auditing laws, rules, and regulations:

8.1 Delivery Receipts
8.2 Sales Invoice / Billing Statement
8.3 Certificate of Acceptance issued by the ICTSS Director
8.4 Training Manual
8.5 As-built Documentation[6]
8.6 NDA

[6] Document redacted before submission to offices outside ICTSS for confidentiality