

PROJECT : ENTERPRISE FIREWALL

A. QUERIES/CLARIFICATIONS RAISED DURING THE PRE-BID CONFERENCE:

	Query/Clarifications	TWG/BAC Reply
1.1	<p>May we clarify whether bidders who have previously secured the bidding documents need to purchase them again?</p> <p>Do we need to return the previous version?</p>	<p>No. Bidders who have previously secured the bidding documents are not required to purchase them again. We will just replace it with the latest bidding documents.</p> <p>No.</p>

B. WRITTEN QUERIES:

	Query/Clarifications	TWG/BAC Reply
2.1	<p>Requirement: (page 97) Bidder must have experience in installation and maintenance of the proposed brand. Must have at least one (1) Installed base each of Head Office and Disaster Recovery (DR) site using the same firewall brand.</p> <p>Bidder must submit list of clients with contact person and contact details - phone and email.</p> <p>Clarification/Request: May we request to relax the requirement to "Bidder must have experience in installation and maintenance of the proposed brand.</p> <p>Bidder must submit list of clients with contact person and contact details - phone and email and Client Satisfactory Survey"?</p>	<p>This will be considered.</p> <p>Bidder must have experience in installation and maintenance of the proposed brand.</p> <p>Bidder must submit list of clients with contact person and contact details - phone and email.</p> <p>This amends Item H. of Bidder Qualification.</p>
2.2	<p>Requirement: (page 96) Bidder must be at least Manufacturer Certified Premier Partner or equivalent and must have specialization in Hyper-Scaling Device Firewall solution for the Head Office Firewall</p>	<p>We maintain the requirement.</p>

	Query/Clarifications	TWG/BAC Reply
	<p>Bidder must submit Manufacturer Certification stating its partnership level and Hyper Scaling device specialization with the proposed firewall.</p> <p>Clarification/Request: May we request to relax the requirement to “Bidder must be at least Authorized Reseller of the Manufacturer.”?</p>	
2.3	<p>Requirement: (page 96) Bidder must have Three (3) Manufacturer Certified Expert for the Head Office Firewall</p> <p>Two (2) Manufacturer Certified Security Expert</p> <p>One (1) Manufacturer Certified Hyper Scale Device Expert</p> <p>Clarification/Request: May we request to relax the requirement to “Bidder must have</p> <p>at least One (1) Manufacturer Certified Expert for the Head Office Firewall</p> <p>at least One (1) Manufacturer Certified Security Expert”?</p>	<p>This will be considered.</p> <p>Bidder must have Two (2) Manufacturer Certified Expert for the Head Office Firewall</p> <p>One (1) Manufacturer Certified Security Expert</p> <p>One (1) Manufacturer Certified Hyper Scale Device Expert</p> <p>This amends Item D. of Bidder Qualification.</p>
2.4	<p>Requirement: (page 96) Bidder must submit valid Project Management Professional Certification, resume, company ID and certificate of employment. Certified Project Manager should be with the bidder two (2) years before the bid opening.</p> <p>Clarification/Request: May we request to relax the requirement to “The PM should be with the bidder for at least 1 year before the bid opening”?</p>	<p>This will be considered.</p> <p>Bidder must submit valid Project Management Professional Certification, resume, company ID and certificate of employment. Certified Project Manager should be with the bidder one (1) year before the bid opening.</p> <p>This amends Item B. of Bidder Qualification.</p>
2.5	<p>Requirement: (page 96) Certified Project Management Professional must have at least Two (2) years experience in Project Management in the Financial Institution industry or other Government Institution.</p>	<p>This will be considered.</p> <p>Certified Project Management Professional must have at least Two (2) years experience in Project Management in any Private or other Government Institution.</p>

	Query/Clarifications	TWG/BAC Reply
	<p>Clarification/Request: May we request to relax the requirement to “Certified Project Management Professional must have at least Two (2) years experience in Project Management in any Private or other Government Institution.”?</p>	<p>This amends Item B. of Bidder Qualification.</p>
2.6	<p>Requirement: (page 96) Bidder must be in network and security system integration for at least ten (10) years in the Philippines</p> <p>Bidder must submit bidder’s certification</p> <p>Clarification/Request: May we request to relax the requirement to “Bidder must have a minimum of ten (10) years of experience in System Integration or ICT-Related business operations in the Philippines.”?</p>	<p>This will be considered.</p> <p>Bidder must have a minimum of ten (10) years of experience in System Integration or ICT-Related business operations in the Philippines.</p> <p>This amends Item A. of Bidder Qualification.</p>
2.7	<p>Requirement: (page 95) Hardware Specifications</p> <ul style="list-style-type: none"> • Storage: 12x 8TB RAID Certified HDD • Interfaces: 2x 100/1000/10000 1x USB port • 1x DB9 console serial port Dual hot-swappable power supplies <p>Clarification/Request: May we request to relax the requirement to “Storage: 96TB Raw RAID Certified HDD</p> <p>Interfaces:</p> <ul style="list-style-type: none"> - 2x 100/1000/10000 - 1x USB Port - 1x DB9 Console serial port”? 	<p>This will be considered.</p> <p>Hardware Specifications</p> <ul style="list-style-type: none"> • Storage: 12 x 8TB or 96TB Raw RAID Certified HDD • Interfaces: <ul style="list-style-type: none"> - 2x 100/1000/10000 - 1x USB port - 1x DB9 console serial port <p>Dual hot-swappable power supplies</p> <p>This amends Item C. No.3 Letter a.i. of LOG SERVER - for Disaster Recovery Site (1 unit) – Hardware Specifications</p>
2.8	<p>Requirement: (page 94) The central manager must support continuous, automated analysis of your firewall rule base and gives specific, actionable recommendations. It identifies unused rules, redundant policies, and suggests converting outdated port-based rules to modern, application based rules.</p>	<p>We maintain the requirement.</p>

	Query/Clarifications	TWG/BAC Reply
	<p>This functionality is built-in and does not require an additional license or separate module.</p> <p>Clarification/Request: May we request to relax the requirement to “The solution must support analysis of your firewall configuration giving actionable recommendations. It should be able to identify configuration weaknesses and best practice violations in your deployment, optimize your deployment by validating unused and redundant policies.”?</p>	
2.9	<p>Requirement: (page 94) The solution must include automated commit recovery and connectivity testing, allowing managed devices to revert to the previous configuration if a pushed update disrupts connectivity with the management platform.</p> <p>Clarification/Request: May we request to relax the requirement to “The solution must support templates with revision control features with the ability to view the history of changes.”?</p>	We maintain the requirement.
2.10	<p>Requirement: (page 93) The proposed solution must detect and prevent credential phishing by controlling the sites to which users can submit corporate credentials based on the site’s URL category.</p> <p>Clarification/Request: May we request to relax the requirement to “The proposed solution must detect and prevent credential phishing by controlling the sites to which users can submit corporate credentials based on the site’s URL category.”?</p>	We maintain the requirement.
2.11	<p>Requirement: (page 92) The proposed solution must be capable of detecting and blocking DNS responses originating from hijacked domains or misconfigured DNS records, including those that may lead to unauthorized</p>	We maintain the requirement.

	Query/Clarifications	TWG/BAC Reply
	<p>redirection, zone takeovers, or exposure to malicious infrastructure.</p> <p>Clarification/Request: May we request to relax the requirement to “The proposed solution must be capable of detecting and blocking DNS responses originating from hijacked domains or misconfigured DNS records, including those that may lead to unauthorized redirection, zone takeovers, or exposure to malicious infrastructure.”?</p>	
2.12	<p>Requirement: (page 92) The proposed solution must be capable of identifying compromised systems by redirecting DNS queries intended for known command and control domains to a controlled sinkhole environment, enabling effective detection and response.</p> <p>Clarification/Request: May we request to relax the requirement to “The proposed solution must have DNS security features that can defend against DNS attacks and encrypts DNS traffic for user privacy. It should also support DNS tunnelling blocking and protection against DNS flood attacks.”?</p>	We maintain the requirement.
2.13	<p>Requirement: (page 92) The proposed solution must utilize machine learning and predictive analytics to detect and block both known and unknown threats within DNS traffic, enhancing protection against evolving attack techniques.</p> <p>Clarification/Request: May we request to relax the requirement to “The proposed solution must support inline malware prevention to detect unknown files and zero-day threats in real-time with sub-second verdicts..”?</p>	We maintain the requirement.
2.14	<p>Requirement: (Page 85) Solution must support up to at least 32 gateways module in hyperscaling set-up</p>	We maintain the requirement.

	Query/Clarifications	TWG/BAC Reply
	Clarification/Request: May we request to relax the requirement to allow a non hyperscaling setup and two chassis-based Firewall that meets the current required throughput?	
2.15	<p>Requirement: (Page 94) The central management must support access through the following: - Web-based using HTTP or HTTPS – Command Line Interface (CLI) via SSH</p> <p>Clarification/Request: May we request to relax the requirement to allow proposing a solution that only allows Web-based management using HTTPS and not Command Line Interface to retain the user-friendliness of the solution?</p>	We maintain the requirement.
2.16	<p>Requirement: (page 92) The proposed next-generation firewall must incorporate advanced AI technologies—including machine learning, adaptive learning, and generative models—to continuously train security models. This capability should enhance the identification of sophisticated and previously unknown malware, DNS-based threats, and malicious URLs, including those generated through AI techniques.</p> <p>Clarification/Request: May we request to relax the requirement to “The proposed solution must utilize machine learning algorithms to detect unknown malware, analyze behavior and characteristics of files to identify and block threats in real-time.”?</p>	We maintain the requirement.
2.17	<p>Requirement: (page 92) The proposed solution shall enable run-time memory monitoring by capturing memory snapshots at crucial instances upon detecting malicious behavior.</p> <p>Clarification/Request: May we request to relax the requirement to “The proposed solution shall support</p>	We maintain the requirement.

	Query/Clarifications	TWG/BAC Reply
	<p>heuristic antivirus engine that can perform tests on files to detect virus-like behavior or known virus indicators.”?</p>	
2.18	<p>Requirement: (Page 90) The proposed solution should utilize a security-centric Operating System, be delivered as a purpose-built appliance rather than generic hardware, and process traffic in a single-pass manner for efficient performance.</p> <p>Clarification/Request: May we request to relax the requirement to allow a solution that uses a generic processor but meets the required Threat Prevention Throughput?</p>	We maintain the requirement.
2.19	<p>Requirement: (page 92) The proposed solution must be capable of detecting and analyzing malicious behavior during malware execution, including in-memory activities, while remaining completely invisible to the program under analysis to prevent malicious actors obfuscating their payloads.</p> <p>1. Requirement: (page 92) The proposed solution must be capable of detecting and analyzing malicious behavior during malware execution, including in-memory activities, while remaining completely invisible to the program under analysis to prevent malicious actors obfuscating their payloads.</p> <p>Clarification/Request: May we request to relax the requirement to “The proposed solution shall support AI-based malware detection that has the ability to detect potentially malicious Windows Portable Executables to mitigate zero-day attacks.”?</p> <p>Clarification/Request: May we request to relax the requirement to “The proposed solution shall support AI-based malware detection that has the</p>	We maintain the requirement.

	Query/Clarifications	TWG/BAC Reply
	ability to detect potentially malicious Windows Portable Executables to mitigate zero-day attacks.”?	
2.20	<p>Requirement: (Page 94) The central management shares a near-identical user interface and a common management paradigm with the individual NGFW.</p> <p>Clarification/Request: May we request to relax the requirement to allow a solution that does not share a near-identical user interface with the individual NGFW but provides consistent management experience using aligned concepts, terminology, and policy workflows.</p>	We maintain the requirement.
2.21	<p>Requirement: (Page 95) The proposed firewall to be installed at the Disaster Recovery Site should not be the same as the one deployed at the Head Office.</p> <p>Clarification/Request: May we request to relax the requirement to allow proposing the same brand and model to be deployed at the Head Office to allow using a single Central Management solution?</p>	We maintain the requirement.
2.22	<p>Requirement: (Page 97) Bidder must have Two (2) Manufacturer Certified Engineer for the proposed DR Firewall</p> <p>Clarification/Request: May we request to relax the requirement to the “Bidder must have One (1) Manufacturer Certified Engineer for the proposed DR Firewall.”?</p>	<p>This will be considered.</p> <p>Bidder must have One (1) Manufacturer Certified Engineer for the proposed DR Firewall</p> <p>This amends Item F. of Bidder Qualification</p>