DEPARTMENT OF FOREIGN AFFAIRS

BIDS AND AWARDS COMMITTEE
2330 Roxas Boulevard, Pasay City
Tel. Nos. 834-4823; Fax No. 831-9584
Email: bac.secretariat@dfa.gov.ph

SUPPLEMENTAL / BID BULLETIN No. 1

Project	:	Procurement of Firewall/ Unified Threat Management Appliance (Secondary Cybersecurity Solution)
Reference No.	:	PB-GS-07-2016
ABC	:	PhP 13,500,000.00
Date	:	11 August 2017

This supplemental/bid bulletin is issued to provide information to the prospective proponents/bidders on the following changes to the Bidding Documents:

I. Invitation to Bid (Section I)

1. Bidders should have completed, within the past ~~five (5)~~ **ten (10)** years from the date of submission and receipt of bids, a contract similar to the Project. The description of an eligible bidder is contained in the Bidding Documents, particularly, in Section II, Instructions to Bidders.

5. The DFA-BAC has scheduled the following activities for the said Project:

2nd Pre-bid	**Deadline for Submission and Receipt of Bids**	**Bid Opening**
16 August 2017, Wednesday, 2:00 p.m.	**29 ~~14~~ August 2017,** **Tuesday** ~~Monday~~, 12:00 n.n.	**29 ~~14~~ August 2017,** **Tuesday** ~~Monday~~, 2:30 p.m.
Venue: Bids and Awards Committee (BAC) Conference Room, 12th Floor, DFA Main Building, Roxas Boulevard, Pasay City		

The DFA-BAC will hold a Pre-Bid Conference on the above-stated date, which shall be open to all interested bidders.

II. Technical Specifications (Section VII)

The Technical Specifications (Section VII) of the Bidding Documents is superseded by **ANNEX A** of this Supplemental/Bid Bulletin No. 1.

The Bidding Documents is amended accordingly.

For the information and guidance of all concerned.

(Sgd.)
MARIA TERESA C. LEPATAN
BAC Chairperson

ANNEX A

Technical Specifications

FIREWALL/UNIFIED THREAT MANAGEMENT APPLIANCE
(SECONDARY CYBERSECURITY SOLUTION)

I.	**BACKGROUND**		
	The Department of Foreign Affairs (DFA) is the primary government agency implementing the Philippines' foreign policy. In working for the country's best interests in international relations, as well as providing services and protection for Filipinos abroad, the DFA maintains more than eighty-five embassies and consulate offices abroad (Foreign Service Posts / FSPs), twenty-one regional consular offices (RCOs) and several passport satellite offices (SOs) in the Philippines. The DFA Home Office serves as the central hub for administrative oversight and management of its Foreign Service Posts and regional offices, all of which rely on data, voice and software applications in order to perform its day-to-day activities, interacting with public clients as well as various inter-office transactions among its nearly 3,000 personnel.		
II.	**OBJECTIVE**		
	The Department of Foreign Affairs requires technical equipment to support the interconnectivity between its various local and foreign offices, enabling various network services, telephony, current database applications and future information systems to be made available to remote sites and roaming users. To meet this target of providing security, site-to-site integration and connectivity, while ensuring protection from network intrusion, cyber attacks, malware, application-level strikes, backdoor threats, Trojans, and other internet-borne threats, the DFA seeks to acquire a comprehensive network security multifunction firewall/unified threat management package. It should meet its present and future needs within the approved budget of Thirteen Million Five Hundred Thousand Pesos (PhP 13,500,000.00) -- equipment, installation, training and all necessary licensing fees, and lawful taxes included.		
III.	**SCOPE**		**Statement of Compliance**
A.	**EQUIPMENT TYPE**		
	Target Deployment	**Quantity**	
	Large enterprise / central office requiring high performance features to support approximately 1,500 host machines, 100 simultaneous site-to-site VPN connections, more than 200 roaming VPN clients.	**2**	
	Medium-size distributed office / branch office of about 500 host machines, 50 simultaneous site-to-site VPN connections, 50 roaming VPN clients	**6**	
	Stand-alone distributed offices of less than 100 host machines	**46**	
	TOTAL	**54**	

B.	**TECHNICAL SPECIFICATIONS**		
	Target Deployment: LARGE ENTERPRISE (DFA Main Office)		
	Feature	**Minimum Specification**	
	VPN	Supports Internet Protocol Security (IPSec), Secure Sockets Layer (SSL) , Transport Layer Security (TLS) protocols for site-to-site and/or remote site connections	
		Capable of at least 1Gbps throughput	
	Traffic Shaping and Application Filtering	Supports bandwidth restriction with rule-sets for traffic categories and Open Systems Interconnection (OSI) model Layer 7 application control and analysis.	
	Firewall	Capable of rule-set definitions to pass/allow inbound and outbound traffic by protocol type, port number, etc, using stateful packet inspection	
	Intrusion Prevention/Intrusion Detection System	Capable of intelligent packet inspection for IPS/IDS detected threats plus integrated report generation.	
		Capable of at least 1Gbps throughput	
	Web cache and URL filtering	Capable of blocking specific Uniform Resource Locater (URLs) or categories of websites, with day/time scheduling	
		With report generation of corresponding web sites blocked/visited with time period summaries or per user/group access	
	Anti-virus	Integrated AV checking for inbound/outbound data and http traffic, with integrated report generation for threats	
		Capable of at least 1Gbps AV throughput	
	User authentication	Supports Lightweight Directory Access Protocol (LDAP), Active Directory, Radius, local database user list for authentication	
		Two-factor authentication capable	
	Concurrent connections	Supports at least 1 Million concurrent connections	
	Multi-WAN	Supports load-balancing and fail-over for multiple ISP Wide Area Network (WAN) configuration	
		(minimum of 2 WAN ports)	

	Local storage	Hot-swappable, RAID-enabled Serial ATA/Solid State Drive (SSD) (at least 240 Gigabytes of space)	
	Network Interface and expansion	Minimum of 16 ports for Local Area Network (LAN) at Gigabit speed, with support for fiber-optic interface module included (at least 2 available)	
	I/O ports	1 x VGA	
		At least 1 USB 2.0 / USB 3.0 port	
		1 x COM/console/management port	
	Mounting	Rack-mountable (inclusive of rails)	
	Power	Redundant, 2x hot-swappable auto-volt power supply (100-240 VAC)	
	Certifications	Gartner-certified Leading product in UTM category at least two times from 2011-2016.	
	Device Management/Configuration and Alerts	Browser-based, centralized, integrated management interface for configuration and real-time status monitoring of the firewall/UTM across multiple sites. Functionality shall include capability to view networked nodes, bandwidth, application usage and pushing of template-enabled security policy configurations across multiple devices in the enterprise securely over the internet.	
		Supports alert-sending and report submission via email	
	Reports and Statistics	Supports generation of time-specific service-related reports and user/data/traffic statistics.	
	Throughput	Performs at the specified minimum throughput indicated in each feature set concurrent with other services running at full capacity.	
	Target Deployment: MEDIUM ENTERPRISE (ASEANA)		
	Features	**Minimum Specification**	
	VPN	Supports IPSEc, SSL, TLS protocols for site-to-site and/or remote site connections	
		Capable of at least 1Gbps throughput	
	Traffic Shaping and Application Filtering	Supports bandwidth restriction with rule-sets for traffic categories and Open Systems Interconnection (OSI) model Layer 7 application control and analysis.	
	Firewall	Capable of rule-set definitions to pass/allow inbound and outbound traffic by protocol type, port number, etc, using stateful packet inspection	

	Intrusion Prevention/Intrusion Detection System	Capable of intelligent packet inspection for IPS/IDS detected threats plus integrated report generation.	
		Capable of at least 1Gbps throughput	
	Web cache and URL filtering	Capable of blocking specific URLs or categories of websites, with day/time scheduling	
		With report generation of corresponding web sites blocked/visited with time period summaries or per user/group access	
	Anti-virus	Integrated AV checking for inbound/outbound data and http traffic, with integrated report generation for threats	
		Capable of at least 1Gbps AV throughput	
	User authentication	Supports LDAP, Active Directory, Radius, local database user list for authentication	
		Two-factor authentication capable	
	Concurrent connections	Supports at least 1 Million concurrent connections	
	Multi-WAN	Supports load-balancing and fail-over for multiple ISP configuration	
		(minimum of 2 WAN ports)	
	Local storage	Hot-swappable, RAID-enabled Serial ATA /SSD (at least 240 Gigabytes of space)	
	Network Interface and expansion	Minimum of 12 ports for LAN at Gigabit speed, with support for fiber-optic interface module included (at least 2 available)	
	I/O ports	1 x VGA	
		At least 1 USB 2.0 / USB 3.0 port	
		1 x COM/console/management port	
	Mounting	Rack-mountable (inclusive of rails)	
	Power	Redundant, 2x hot-swappable auto-volt power supply (100-240 VAC)	
	Certifications	Gartner-certified Leading product in UTM category at least two times from 2011-2016.	
	Device Management/Configuration and Alerts	Browser-based, centralized, integrated management interface for configuration and real-time status monitoring of the firewall/UTM across multiple sites. Functionality shall include capability to view networked nodes, bandwidth, application usage and pushing of template-enabled security policy configurations across multiple devices in the enterprise securely over the internet.	

		Supports alert-sending and report submission via email	
	Reports and Statistics	Supports generation of time-specific service-related reports and user/data/traffic statistics.	
	Throughput	Performs at the specified minimum throughput indicated in each feature set concurrent with other services running at full capacity.	
	Target Deployment: Small Office (FSPs/RCOs/SOs)		
	Features	**Minimum Specification**	
	VPN	Supports IPSEc, SSL, TLS protocols for site-to-site and/or remote site connections	
		Capable of at least 200Mbps throughput	
	Traffic Shaping and Application Filtering	Supports bandwidth restriction with rule-sets for traffic categories and Open Systems Interconnection (OSI) model Layer 7 application control and analysis.	
	Firewall	Capable of rule-set definitions to pass/allow inbound and outbound traffic by protocol type, port number, etc, using stateful packet inspection	
	Intrusion Prevention/Intrusion Detection System	Capable of intelligent packet inspection for IPS/IDS detected threats plus integrated report generation.	
		Capable of at least 300Mbps throughput	
	Web cache and URL filtering	Capable of blocking specific URLs or categories of websites, with day/time scheduling	
		With report generation of corresponding web sites blocked/visited with time period summaries or per user/group access	
	Anti-virus	Integrated AV checking for inbound/outbound data and http traffic, with integrated report generation for threats	
		Capable of at least 300Mbps AV throughput	
	User authentication	Supports LDAP, Active Directory, Radius, local database user list for authentication	
		Two-factor authentication capable	
	Concurrent connections	Supports at least 500,000 concurrent connections	
	WAN port	*At least* 1 ethernet port for WAN interface	

	Local storage	Flash-based on-board storage (at least 64 Gigabytes of flash or SSD storage)	
	Network Interface and expansion	Minimum of 2 ports for LAN at Gigabit speed	
	I/O ports	At least 1 USB port	
		1 x COM/console/management port	
	Mounting	Stand-alone or rack-mountable (inclusive of rails)	
	Power	Auto-volt power supply (100-240 VAC)	
	Certifications	Gartner-certified Leading product in UTM category at least two times from 2011-2016.	
	Device Management/Configuration and Alerts	Browser-based, centralized, integrated management interface for configuration and real-time status monitoring of the firewall/UTM across multiple sites. Functionality shall include capability to view networked nodes, bandwidth, application usage and pushing of template-enabled security policy configurations across multiple devices in the enterprise securely over the internet.	
		Supports alert-sending and report submission via email	
	Reports and Statistics	Supports generation of time-specific service-related reports and user/data/traffic statistics.	
	Throughput	Performs at the specified minimum throughput indicated in each feature set concurrent with other services running at full capacity.	
IV.	**TRAINING**		
	A knowledge transfer training not exceeding five (5) days for ten (10) OAMSS-ITRD personnel shall be conducted by the Contractor at least thirty (30) calendar days prior to equipment delivery. The training shall properly orient and expose ITCRD personnel to the various features, services, and capabilities of the Firewall/UTM appliance, enabling them to perform basic network administration, device monitoring, configuration of essential VPN settings and appliance security features, deployment, and 1st level troubleshooting. Original English product/equipment brochures/technical manuals/user guides shall be provided per unit for the perusal and records of the DFA, inclusive of any installation media/software application/drivers/etc. from the product manufacturer. Any and all expenses related to the knowledge transfer and equipment training for OAMSS-ITCRD personnel for the duration of the training period shall be borne by the Contractor. The training shall be conducted whenever possible, within the premises of the DFA.		
V.	**CONTRACTOR QUALIFICATION**		

	1. The Contractor shall have at least ten (10) years of experience in supply, delivery, installation, testing and commissioning of network security appliances. The Contractor shall submit proof (as stated in its Articles of Incorporation) that the primary purpose of their enterprise is to provide the technical/Information and Communications Technology equipment and corresponding services.	
	2. The Contractor shall submit the following issued by the manufacturer of the FIREWALL/UNIFIED THREAT MANAGEMENT APPLIANCE: a. A certification endorsing the Contractor, to bid, sell, support & maintain the product being offered	
	b. A certification attesting to the fact that the Contractor provides after sales service and parts/stocks of the required equipment, accessories and software included in this project, covering the next 5 years commencing from the date of bid submission. The certification shall include company names, addresses and proper contacts.	
	c. A certification that all equipment and software being offered by the Contractor are non-refurbished, brand new and up-to-date.	
	d. A certification that the Contractor is a Certified Partner for the brand/appliance for at least five (5) consecutive years.	
	e. A certification that the Contractor's technical support personnel have acquired the necessary proficiency, expertise and experience qualifying them to fully support the FIREWALL/UNIFIED THREAT MANAGEMENT APPLIANCE being offered.	
	3. The Contractor's organic, in-house employed network engineers shall have the following minimum qualifications for proper support and installation of the FIREWALL/UNIFIED THREAT MANAGEMENT APPLIANCE: a. Cisco Certified Network Associate (CCNA) b. Cisco Certified Design Associate (CCDA)	
VI.	**TECHNICAL SUPPORT AND WARRANTY**	
	1. The Contractor shall provide full hardware warranty during the duration of the contract. Defective or malfunctioning equipment locally deployed within the Philippines shall be promptly replaced within three (3) working days from the date of formal notification by OAMSS-ITCRD, at no expense to the Department of Foreign Affairs. Replacements for units deployed abroad shall be delivered to OAMSS-ITCRD within five (5) work days from the date of formal notification by the DFA.	

	2. The Contractor shall provide 24x7 technical/customer support for OAMSS-ITCRD, four (4) hours response and six (6) hours resolution time the duration of the contract.	
VII.	**DELIVERY AND PAYMENT**	
	1. The Contractor shall deliver and provision a fully functional and properly-configured Firewall/Unified Threat Management Appliance product within sixty (60) calendar days upon receipt of Notice to Proceed (NTP). Delivery of all units shall be at the 10th Floor OAMSS-ITCRD Department of Foreign Affairs, 2330 Roxas Boulevard, Pasay City, between 9:00 a.m.- 5:00 p.m. The Contractor shall notify the Department of Foreign Affairs in writing of equipment arrival at least one (1) day before the scheduled delivery date to OAMSS-ITCRD, providing the necessary particulars as to the delivery vehicle(s) and accompanying support personnel.	
	2. Payments shall be made thirty (30) working days upon full implementation of the system and receipt of the invoice with complete requirements through List of Due and Demandable Accounts Payable (LDDAP). The list of documentary requirements needed for payment will be provided by the Office of Financial Management Services-Financial Resource Management Division (OFMS-FRMD) upon signing of the contract	

Note:

Bidder must state compliance to each of the provisions in the Terms of Reference/Technical Specifications, as well as to the Schedule to Requirements. The **STATEMENT OF COMPLIANCE** must be signed by the authorized representative of the Bidder, with proof of authority to sign and submit the bid for and in behalf of the Bidder concerned. If the Bidder is a joint venture, the representative must have authority to sign for and in behalf of the partners to the joint venture.

Conformé:

[Signature/s]

[Name of Bidder's Authorized Representative/s]

[Date]