Supplemental/ Bid Bulletin No. 2
June 11, 2019

PUBLIC BIDDING No. 19-168– 1

SUPPLY, DELIVERY, INSTALLATION, TESTING, TRAINING AND COMMISSIONING OF NEXT GENERATION FIREWALL APPLIANCE FOR

TECHNICAL EDUCATION SKILLS AND DEVELOPMENT AUTHORITY (TESDA)

Issued pursuant to Sec. 22.5 of the IRR of R.A. 9184 to clarify and/or amend certain provisions in the Bidding Documents issued for this project, considering the issues raised and clarifications made by prospective bidders during the Pre-Bid Conference held on **June 04, 2019.**

A. AMENDMENTS

REFERENCE	BASES FOR AMENDMENT / INCLUSION
SECTION V: SPECIAL CONDITIONS OF THE CONTRACT	
Page 63 **Contact Person:** Mr. Manuel T. Pili/Mr. Oscar Ruma, Jr. ~~811-3499/817-2529/~~893-8281	*To update the end-user agency's contact number.*
SECTION VII. TECHNICAL SPECIFICATIONS	

		To effect change as approved by the Bids and Awards Committee (BAC) with concurrence of the End-User Agency, please see attached "Appendix 1" for the revised Section VII. Technical Specifications Form.
AGENCY SPECIFICATIONS	**BIDDER'S STATEMENT OF COMPLIANCE**	
Next Generation Firewall Appliance *Complies with the following minimum requirements:*	Brand and Model:	
Hardware Specifications		
• Ethernet Interfaces: 8 GE copper; 2 10GbE SFP+		
• ~~Flexi Port Modules: 8 port GE copper; 8 port GE SFP; 4 port 10 GE SFP+~~		

• Storage 2 x ~~*240 GB~~ *Integrated* SSD		
• ~~RAM 16GB DD4~~		
Performance		
• Firewall Throughput: ~~40 to 50 Gbps~~ *At least 50 Gbps*		
• VPN Throughput: ~~5 to 6 Gbps~~ *At least 5 Gbps*		
• IPS Throughput: ~~9 to 10 Gbps~~ *At least 10 Gbps*		
• ~~NGFW (IPS + Apps): 6.5 to 7.5 Gbps~~		
• ~~Anti Virus Throughput (Proxy): 6 to 7 Gbps~~		
• Concurrent Connections: ~~15,000,000 to 20,000,000~~ *At least 20,000,000*		
• New Connections/sec: ~~190,000 to 200,000~~ *At least 200,000*		
• Maximum Licensed Users: unrestricted		
Physical Specifications		
• ~~Dimensions: 16in to 18in (W) x 18in to 20in (L) x 1in to 2in (H) (Width x Length x Height)~~		
• ~~Weight: 7-9 kg / 17-18 lbs (unpacked) 14-15 kg / 32-34 lbs (packed)~~		
• Mounting: 1U (rack mount, ~~sliding rails must be included)~~		
• Power Consumption: ~~31W, 107 BTU/hr (idle) 83W, 283 BTU/hr (full load)~~ *At least 31W*		
• ~~Operating temperature: 0-40°C (operating) -20 to +80°C (storage)~~		
• ~~Humidity: 10% to 90%, Non-condensing~~		
~~**Product Certifications:** CB, UL, CE, FCC Class A, ISED, VCCI, RCM, CCC, KC, BIS~~		
~~**Physical Interfaces**~~		
• ~~Hard Drive (Local quarantine/logs): 2x Integrated SSD~~		
• ~~Ethernet Interfaces: 8 GE copper (incl 2 bypass pairs); 2 10GbE SFP+~~		
• ~~No of Flexi Port slots: 2~~		
• ~~I/O Ports: 2x USB 3.0; 1 Micro USB;~~		

~~1x COM Port (RJ45); 1x HDMI port~~	
• ~~Display: Multi-functional LCD Module~~	
• ~~Power Supply: Internal auto-ranging 110-240VAC, 50-6- Hz Hot Swap Redundant PSU Optional~~	
General Management	
• Purpose-built streamlined user interface and firewall rule management for large rule sets with grouping with at-a-glance rule feature and enforcement indicators	
• Two-factor authentication (One-time-password) support for administrator access, user portal, IPSec and SSL VPN	
• Advanced trouble-shooting tools in GUI (e.g., Packet Capture)	
• High Availability (HA) support clustering two devices in active-active or active-passive mode.	
• Full command-line-interface (CLI) accessible from GUI	
• Role-based administration	
• Automated firmware update notification with easy automated update process and roll-back features	
• Reusable system object definitions for networks, services, hosts, time periods, users and groups, clients and servers	
• Self-service user portal	
• Configuration change tracking	
• Flexible device access control for services by zones	
• Email or SNMP trap notification options	
Firewall, Networking, and Routing	
• Stateful deep packet inspection firewall	
• FastPath Packet Optimization	
• User, group, time, or network based policies	
• Access time polices per user/group	

• Enforce policy across zones, networks, or by service type		
• Zone isolation and zone-based policy support.		
• Default zones for LAN, WAN, DMZ, LOCAL, VPN, and WiFi		
• Custom zones on LAN or DMZ		
• Customizable NAT policies with IP masquerading and full object support to redirect or forward multiple services in a single rule		
• Flood protection: DoS, DDoS and portscan blocking		
• Country blocking by geo-IP		
• Routing: static, multicast (PIM-SM) and dynamic (RIP, BGP, OSPF)		
• Upstream proxy support		
• Protocol independent multicast routing with IGMP snooping		
• Bridging with STP support and ARP broadcast forwarding		
• VLAN DHCP support and tagging		
• Multiple bridge support		
• ~~WAN link balancing: multiple Internet connections, auto-link health check, automatic failover, automatic and weighted balancing, and granular multipath rules~~		
• ~~Wireless WAN support (n/a in virtual deployments)~~		
• ~~802.3ad interface link aggregation~~		
• ~~Full configuration of DNS, DHCP and NTP~~		
• ~~Dynamic DNS~~		
• ~~IPv6 Ready Logo Program Approval Certification~~		
• ~~IPv6 tunneling support including 6in4, 6to4, 4in6, and IPv6 rapid deployment (6rd) through IPSec~~		
Base Traffic Shaping and Quotas		
• Flexible network or user-based traffic shaping (QoS) (enhanced Web and App traffic shaping options are included with the Web Protection Subscription)		
• Set user-based traffic quotas on upload/download or total traffic and cyclical or non-cyclical		

• Real-time VoIP optimization	
• DSCP marking	
~~Secure Wireless~~	
• ~~Simple plug-and-play deployment of wireless access points (APs) — automatically appear on the firewall~~	
• ~~Central monitor and manage all APs and wireless clients through the built-in wireless controller~~	
• ~~Bridge APs to LAN, VLAN, or a separate zone with client isolation options~~	
• ~~Multiple SSID support per radio including hidden SSIDs~~	
• ~~Support for the latest security and encryption including WPA2 Personal and Enterprise~~	
• ~~Channel width selection option~~	
• ~~Support for IEEE 802.1X (RADIUS authentication)~~	
• ~~Support for 802.11r (fast transition)~~	
• ~~Hotspot support for (custom) vouchers,~~	
• ~~password of the day, or T&C acceptance~~	
• ~~Wireless guest Internet access with walled garden options~~	
• ~~Time-based wireless network access~~	
Authentication	
• Transparent, proxy authentication (NTLM/Kerberos) or client authentication	
• Authentication via: Active Directory, eDirectory, RADIUS, LDAP and TACACS+	
• Server authentication agents for Active	
• Directory SSO, STAS, SATC	
• Client authentication agents for Windows, Mac OS X, Linux 32/64	
• Authentication certificates for iOS and Android	
• Single sign-on: Active directory, eDirectory	
• Authentication services for IPSec,	

L2TP, PPTP, SSL	
• Captive Portal	
~~User Self-Serve Portal~~	
• ~~Download SSL remote access client (Windows) and configuration files (other OS)~~	
• ~~Hotspot access information~~	
• ~~Change user name and password~~	
• ~~View personal internet usage~~	
• ~~Access quarantined messages and manage user-based~~	
• ~~Block/allow sender lists (requires Email Protection)~~	
Base VPN Options	
• Site-to-site VPN: SSL, IPSec, 256-bit AES/3DES, PFS, RSA, X.509 certificates, pre-shared key	
• L2TP and PPTP	
• Remote access: SSL, IPsec, iPhone/iPad/Cisco/Andriod VPN client support	
• IKEv2 Support	
• SSL client for Windows and configuration download via user portal	
Intrusion Prevention (IPS)	
• High-performance, next-gen IPS deep packet inspection engine with selective IPS patterns that can be applied on a firewall rule basis for maximum performance and protection	
• Top rated by NSS Labs	
• Thousands of signatures	
• Support for custom IPS signatures	
• IPS Policy Smart Filters that enable dynamic policies which automatically update as new patterns are added	
Web Protection and Control	
• Fully transparent proxy for anti-malware and web-filtering	
• Enhanced Advanced Threat Protection	
• URL Filter database with millions of sites across 92 categories	

• Surfing quota time policies per user/group		
• Access time polices per user/group		
• Malware scanning: block all forms of viruses, web malware, trojans, and spyware on HTTP/S, FTP and web-based email		
• Advanced web malware protection with JavaScript emulation		
• Live Protection real-time, in-the-cloud lookups for the latest threat intelligence		
• Second independent malware detection engine for dual-scanning		
• Real-time or batch mode scanning		
• Pharming Protection		
• HTTP and HTTPS scanning and enforcement on any network and user policy with fully customizable rules and exceptions		
• SSL protocol tunneling detection and enforcement		
• Certificate validation		
• High performance web content caching		
• File type filtering by mime-type, extension and active content types (e.g. Activex, applets, cookies, etc.)		
~~Email Protection and Control~~		
• ~~E-mail scanning with SMTP, POP3, and IMAP support~~		
• ~~Block spam and malware during the SMTP transaction~~		
• ~~Spam greylisting~~		
• ~~Recipient verification for mistyped email addresses~~		
• ~~Second independent malware detection engine for dual-scanning~~		
• ~~Live Protection real-time, in-the-cloud lookups for the latest threat intelligence~~		
• ~~Automatic signature and pattern updates~~		
• ~~Smart host support for outbound relays~~		
• ~~File Type detection/blocking/scanning of attachments~~		

~~- Accept, reject or drop over-sized messages~~		
~~- Detects phishing URLs within e-mails~~		
~~- Use pre-defined content scanning rules or create your own custom rules based on a variety of criteria with granular policy options and exceptions~~		
~~- TLS Encryption support for SMTP, POP, and IMAP~~		
~~- Append signature automatically to all outbound messages~~		
~~- Email archiver~~		
~~- Individual user-based block and allow sender lists maintained through the user portal~~		
Web Application Firewall Protection		
• Reverse proxy		
• URL hardening engine with deep-linking and directory traversal prevention		
• Form hardening engine		
• SQL injection protection		
• Cross-site scripting protection		
• Dual-antivirus engines		
• HTTPS (SSL) encryption offloading		
• Cookie signing with digital signatures		
• Path-based routing		
• Outlook anywhere protocol support		
• Reverse authentication (offloading) for form-based and basic authentication for server access		
• Virtual server and physical server abstraction		
• Integrated load balancer spreads visitors across multiple servers		
• Skip individual checks in a granular fashion as required		
~~1 Unit Access-Point Capacity~~		
~~- Maximum throughput: 867 Mbps + 300 Mbps~~		
~~- Multiple SSIDs: 8 per radio (16 in total)~~		

~~**Technical Specifications**~~		
• ~~LAN interface: 1 x 10/100/1000 Base TX~~		
• ~~Supported WLAN Standards: 802.11 a/b/g/n/ac 2.4 and 5 GHz~~		
• ~~Power over Ethernet (min.): 802.3at~~		
• ~~Number of antennas: 2 external~~		
• ~~MIMO capabilities: 2x2:2~~		
~~**Physical Specifications**~~		
• ~~Dimensions (WxHxD): 180-185 x 33-36 x 180-183 mm~~		
• ~~Weight: 500-550g~~		
• ~~Mounting options: Desktop/wall~~		
Other Requirements:		
• Must have at least one (1) Certified Solutions Engineer / Solutions Architect of the solutions being offered		
• Must be Authorized Partner of the Solutions being offered		
• 3 years Hardware Warranty Certificate from the Company of the solution being offered		
• ~~Unlimited access to Online Forum~~		
• 2 days Comprehensive Training for ~~10~~ 5 personnel		
• ~~Quarterly Health Check / Visit~~		
• ~~User Awareness Seminar (2x sessions for 1 day)~~		

All other portions of the Bidding Documents affected by these amendments shall be made to conform to the same.

Amendments/inclusions/clarifications made herein shall be considered an integral part of the Bidding Documents.

The changes made in the Philippine Bidding Documents (5th Edition, August 2016) are deemed integrated in the terms and conditions for this project.

-SGD-
ENGR. ROSANA D. YAMBAO
Chairperson, DBM-PS BAC I

"Appendix 1"

Technical Specifications

Supply, Delivery, Installation, Testing, Training and Commissioning of Next Generation Firewall Appliance

QUANTITY : 1 lot

APPROVED BUDGET FOR THE CONTRACT : ₱1,880,000.00

AGENCY SPECIFICATIONS	BIDDER'S STATEMENT OF COMPLIANCE
Next Generation Firewall Appliance *Complies with the following minimum requirements:*	Brand and Model:
Hardware Specifications	
• Ethernet Interfaces: 8 GE copper; 2 x 10GbE SFP+ • Storage: 2 x Integrated SSD	
Performance	
• Firewall Throughput: At least 50 Gbps • VPN Throughput: At least 5 Gbps • IPS Throughput: At least 10 Gbps • Concurrent Connections: At least 20,000,000 • New Connections/sec:At least 200,000 • Maximum Licensed Users: unrestricted	
Physical Specifications	
• Mounting: 1U (rack mount) • Power Consumption: At least 31W	
General Management	
• Purpose-built streamlined user interface and	

firewall rule management for large rule sets with grouping with at-a-glance rule feature and enforcement indicators	
• Two-factor authentication (One-time-password) support for administrator access, user portal, IPSec and SSL VPN	
• Advanced trouble-shooting tools in GUI (e.g., Packet Capture)	
• High Availability (HA) support clustering two devices in active-active or active-passive mode.	
• Full command-line-interface (CLI) accessible from GUI	
• Role-based administration	
• Automated firmware update notification with easy automated update process and roll-back features	
• Reusable system object definitions for networks, services, hosts, time periods, users and groups, clients and servers	
• Self-service user portal	
• Configuration change tracking	
• Flexible device access control for services by zones	
• Email or SNMP trap notification options	
Firewall, Networking, and Routing	
• Stateful deep packet inspection firewall	
• FastPath Packet Optimization	
• User, group, time, or network based policies	
• Access time polices per user/group	
• Enforce policy across zones, networks, or by service type	
• Zone isolation and zone-based policy support.	
• Default zones for LAN, WAN, DMZ, LOCAL, VPN, and WiFi	
• Custom zones on LAN or DMZ	
• Customizable NAT policies with IP masquerading and full object support to redirect or forward multiple services in a single rule	
• Flood protection: DoS, DDoS and portscan blocking	
• Country blocking by geo-IP	
• Routing: static, multicast (PIM-SM) and dynamic (RIP, BGP, OSPF)	
• Upstream proxy support	
• Protocol independent multicast routing with IGMP snooping	

• Bridging with STP support and ARP broadcast forwarding	
• VLAN DHCP support and tagging	
• Multiple bridge support	
Base Traffic Shaping and Quotas	
• Flexible network or user-based traffic shaping (QoS) (enhanced Web and App traffic shaping options are included with the Web Protection Subscription)	
• Set user-based traffic quotas on upload/download or total traffic and cyclical or non-cyclical	
• Real-time VoIP optimization	
• DSCP marking	
Authentication	
• Transparent, proxy authentication (NTLM/Kerberos) or client authentication	
• Authentication via: Active Directory, eDirectory, RADIUS, LDAP and TACACS+	
• Server authentication agents for Active	
• Directory SSO, STAS, SATC	
• Client authentication agents for Windows, Mac OS X, Linux 32/64	
• Authentication certificates for iOS and Android	
• Single sign-on: Active directory, eDirectory	
• Authentication services for IPSec, L2TP, PPTP, SSL	
• Captive Portal	
Base VPN Options	
• Site-to-site VPN: SSL, IPSec, 256- bit AES/3DES, PFS, RSA, X.509 certificates, pre-shared key	
• L2TP and PPTP	
• Remote access: SSL, IPsec, iPhone/iPad/Cisco/Andriod VPN client support	
• IKEv2 Support	
• SSL client for Windows and configuration download via user portal	
Intrusion Prevention (IPS)	
• High-performance, next-gen IPS deep packet inspection engine with selective IPS patterns that can be applied on a firewall rule basis for maximum performance and protection	
• Top rated by NSS Labs	

• Thousands of signatures	
• Support for custom IPS signatures	
• IPS Policy Smart Filters that enable dynamic policies which automatically update as new patterns are added	
Web Protection and Control	
• Fully transparent proxy for anti-malware and web-filtering	
• Enhanced Advanced Threat Protection	
• URL Filter database with millions of sites across 92 categories	
• Surfing quota time policies per user/group	
• Access time polices per user/group	
• Malware scanning: block all forms of viruses, web malware, trojans, and spyware on HTTP/S, FTP and web-based email	
• Advanced web malware protection with JavaScript emulation	
• Live Protection real-time, in-the-cloud lookups for the latest threat intelligence	
• Second independent malware detection engine for dual-scanning	
• Real-time or batch mode scanning	
• Pharming Protection	
• HTTP and HTTPS scanning and enforcement on any network and user policy with fully customizable rules and exceptions	
• SSL protocol tunneling detection and enforcement	
• Certificate validation	
• High performance web content caching	
• File type filtering by mime-type, extension and active content types (e.g. Activex, applets, cookies, etc.)	
Web Application Firewall Protection	
• Reverse proxy	
• URL hardening engine with deep-linking and directory traversal prevention	
• Form hardening engine	
• SQL injection protection	
• Cross-site scripting protection	
• Dual-antivirus engines	
• HTTPS (SSL) encryption offloading	
• Cookie signing with digital signatures	
• Path-based routing	
• Outlook anywhere protocol support	
• Reverse authentication (offloading) for form-	

based and basic authentication for server access	
• Virtual server and physical server abstraction	
• Integrated load balancer spreads visitors across multiple servers	
• Skip individual checks in a granular fashion as required	
Other Requirements:	
• Must have at least one (1) Certified Solutions Engineer / Solutions Architect of the solutions being offered	
• Must be Authorized Partner of the Solutions being offered	
• 3 years Hardware Warranty Certificate from the Company of the solution being offered	
• 2 days Comprehensive Training for 5 personnel	

I hereby certify that the statement of compliance to the foregoing technical specifications are true and correct, otherwise, if found to be false either during bid evaluation or post-qualification, the same shall give rise to automatic disqualification of our bid.

Name of Company / Bidder	Signature Over Printed Name of Authorized Representative	Date