Office of the President of the Philippines
OFFICE OF THE PRESIDENTIAL ADVISER ON THE PEACE PROCESS

REQUEST FOR QUOTATION

27 May 2021

The Office of the Presidential Adviser on the Peace Process (OPAPP) through the General Appropriations Act of FY 2020 intends to apply the sum of Nine Hundred Thousand Pesos (PhP900,000.00) being the Approved Budget for the Contract (ABC) to be paid for the Small Value Procurement, as defined under Section 53.9 of the IRR of RA 9184 for the Procurement of Security Firewall with Remote Access Client listed below:

Lot	Goods	Quantity	Specific Technical Requirements
1	Security Firewall with Remote Access Client	1	See Annex "A"

The OPAPP now invites contractors/suppliers to submit price quotations for the above items.

The Contract will be awarded ***per lot*** to the ***lowest quotation*** and ***responsive*** to the specifications and requirements.

For further inquiries, please coordinate with the BAC Secretariat at telephone number (02) 8636 0706 local 871 or at bacsec.opapp@gmail.com

Sincerely,

Mr. Alain Benedict Ebuen
Head-ICTU

TERMS AND CONDITIONS

a) The ABC is inclusive of applicable taxes, fees, and/or levies payable.
b) The contract shall be awarded to the lowest and responsive bid. Bid amount exceeding the ABC shall be automatically disqualified.
c) The price quotation must be valid for sixty (60) calendar days from the date of submission of bids.
d) Bidder shall submit its quotation and the following documents with all its pages on or before 07 June 2021 at 10:00 AM on the place specified below:

1. Mayor's/Business Permit
2. PhilGEPS Registration Number
3. Omnibus Sworn Statement *(Original Copy)*
4. Latest Income/Business Tax Return

None submission of any or all the document will be declared ineligible to bid and hence, the bid shall be disqualified.

The above documents shall be submitted in a sealed envelope with the name of the sender, complete mailing address, email address, and telephone or mobile number. Without such details, the bid shall not be accepted.

Submit your bidding documents at:

BAC Secretariat Office
3rd Floor, Agustin I Building
F. Ortigas Jr. Road
Ortigas Center
Pasig City

e) Late bids will not be accepted. If you intend to send your bids through a courier, please ensure that we shall receive it before the deadline submission of bids.
f) OPAPP shall conduct evaluation/inspection of goods to be supplied to OPAPP before an award shall be issued.
g) Subcontracting is not allowed.
h) Delivery shall be completed within twenty (20) calendar days from receipt of Job/Purchase Order.
i) Place of Delivery

6th Floor, Agustin I Building
F. Ortigas Jr. Road
Ortigas Center
Pasig City

j) Payment shall be made to the supplier or distributor within thirty (30) calendar days from complete delivery and submission of pertinent documents for payment as required under existing laws.
k) Replacement of defective item/s shall be made within seven (7) days from receipt of the supplier or distributor of the formal written notice.
l) OPAPP reserves the right to reject any and all quotations or bids, declare a failure of bidding or not award the contract in accordance with Section 41 of the IRR of RA 9184.

QUOTATION FORM

OFFICE OF THE PRESIDENTIAL ADVISER ON THE PEACE PROCESS
Agustin I Building
F. Ortigas Jr. Road
Ortigas Center, Pasig City

Dear **Sir/Ma'am**:

After having carefully read and accepted your terms and conditions, we are pleased to quote you for the following items:

Lot	Technical Requirements	Quantity	Statement of Compliance	Unit Cost	Total Cost
1	Security Firewall with Remote Access	1			

Prices in the above offer are certified true and correct.

Sincerely,

_____
(Signature over Printed Name of the Authorized Representative)

Company Name: _____

Contact No: _____

Email Add: _____

Office of the Presidential Adviser on the Peace Process

TERMS OF REFERENCE

Firewall Renewal with Secure Client Devices

TABLE OF CONTENTS

I. PROJECT OVERVIEW

The name of this project is **Firewall Renewal with Secure Client Device**

II. PROJECT OBJECTIVE

The project aims for the renewal of the Firewall at the Office Presidential Adviser on the Peace Process (OPAPP) and the procurement of (2) Secure Client Device to connect branch office to the Ortigas Main Office.

III. TECHNICAL REQUIREMENTS

A. General Requirements

The Project requires for the procurement and subscription of the following:

Item	Quantity	Type	Terms
Firewall Renewal	150	Subscription	Minimum of 1 year
Client Branch Firewall	2	Subscription	1 Year

B. Detailed Technical Requirements (Minimum)

Base Firewall Features	
	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
	SNMP and Netflow support
	Central managment support.

	Backup and restore configurations: locally, via FTP or email; on-demand, daily, weekly or monthly
	Supports API for third party integration
	Firewall, Networking, and Routing
	Stateful deep packet inspection firewall
	Packet Optimization Feature
	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
	802.3ad interface link aggregation
	Full configuration of DNS, DHCP and NTP
	Dynamic DNS
	IPv6 Ready Logo Program Approval Certification
	IPv6 tunnelling 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)
	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 management.
	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) with primary and secondary server support
	Support for 802.11r (fast transition)
	Other Firewall Features
	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
	Wireless repeating and bridging meshed network mode with supported Aps
	Automatic channel selection background optimization
	Support for HTTPS login
	Authentication
	Synchronized User ID utilizes Synchronized Security to share currently logged in Active Directory user ID between endpoints and the firewall without an agent on the AD server or client
	Authentication via: Active Directory, eDirectory, RADIUS, LDAP and TACACS+
	Server authentication agents for Active Directory SSO, STAS, SATC
	Single sign-on: Active directory, eDirectory, RADIUS Accounting
	Client authentication agents for Windows, Mac OS X, Linux 32/64
	Browser SSO authentication: Transparent,proxy authentication (NTLM)
	Browser Captive Portal
	Authentication certificates for iOS and Android
	Authentication services for IPSec, SSL, L2TP, PPTP
	Google Chromebook authentication support for environments with Active Directory and Google Gsuite
	API based authentication
	User Self-Serve Portal
	Download the Authentication Client
	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
	Connect IPSec Client
	Authentication: Pre-Shared Key (PSK), PKI (X.509), Token and XAUTH
	Enables Synchronized Security and Security Heartbeat for remote connected users
	Intelligent split-tunneling for optimum traffic routing
	NAT-traversal support

	Client-monitor for graphical overview of connection status
	Mac and Windows Support
	Network Protection Features
	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
	Granular category selection
	Support for custom IPS signatures
	IPS Policy Smart Filters that enable dynamic policies which automatically update as new patterns are added
	ATP and Security Heartbeat
	Advanced Threat Protection (Detect and block network traffic attempting to contact command and control servers using multi-layered DNS, AFC, and firewall)
	Security heartbeat to instantly identifies compromised endpoints including the host, user, process, incident count, and time of compromise
	Security heartbeat policies can limit access to network resources or completely isolate compromised systems until they are cleaned up
	Lateral Movement Protection further isolates compromised systems by having healthy endpoints reject all traffic from unhealthy endpoints preventing the movement of threats even on the same broadcast domain
	Remote VPN
	Central Management of all remote vpn devices
	Secure encrypted tunnel using digital X.509 certificates and AES256-encryption
	Virtual Ethernet for reliable transfer of all traffic between locations
	IP address management with centrally defined DHCP and DNS Server configuration
	Remotely de-authorize remote vpn devices after a select period of inactivity
	Compression of tunnel traffic
	VLAN port configuration options for hardware option
	Unique encrypted HTML5 self-service portal with support for RDP, HTTP, HTTPS, SSH, Telnet, and VNC
Web Protection Subscription	
	Web Protection and Control
	Fully transparent proxy for antimalware and web-filtering
	URL Filter database with millions of sites across 92 categories, backed by Labs
	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 tunnelling detection and enforcement
	Certificate validation
	File type filtering by mime-type, extension and active content types (e.g. Activex, applets, cookies, etc.)
	YouTube for Schools enforcement per policy (user/group)
	SafeSearch enforcement (DNS-based) for major search engines per policy (user/group)
	Web keyword monitoring and enforcement to log, report or block web content matching keyword lists with the option to upload customs lists
	Block Potentially Unwanted Applications
	Web policy override option for teachers or staff to temporarily allow access to blocked sites or categories that are fully customizable and manageable by select users
	User/Group policy enforcement on Google Chromebooks
	Cloud Application Visibility
	Control Center widget displays amount of data uploaded and downloaded to cloud applications categorized as new, sanctioned, unsanctioned or tolerated
	Discover Shadow IT at a glance
	Drill down to obtain details on users, traffic and data
	One-click access to traffic shaping policies
	Filter cloud application usage by category or volume
	Detailed customizable cloud application usage report for full historical reporting
	Application Protection and Control
	Synchronized App Control to automatically, identify, classify and control all unknown Windows and Mac applications on the network by sharing information between Endpoints and the firewall
	Signature-based application control with patterns for thousands of applications
	Cloud Application Visibility and Control to discover Shadow IT
	App Control Smart Filters that enable dynamic policies which automatically update as new patterns are added
	Micro app discovery and control
	Application control based on category, characteristics (e.g., bandwidth and productivity consuming), technology (e.g., P2P) and risk level
	Per-user or network rule application control policy enforcement
	Web and App Traffic Shaping
	Enhanced traffic shaping (QoS) options by web category or application to limit or guarantee upload/download or total traffic priority and bitrate individually or share
Web Application Subscriptions	
	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
	Match requests from source networks or specified target URLs
	Support for logical and/or operators
	Assists compatibility with various configurations and non-standard deployments
	Options to change Web Appliaction FIrewall performance parameters
	Scan size limit option
	Allow/Block IP ranges
	Wildcard support for server paths
	Automatically append a prefix/suffix for authentication
Sandstorm Protection Subscription	
	Sandstorm Cloud Sandbox Protection
	Full integration into the security solution dashboard
	Inspects executables and documents containing executable content (including .exe, .com, and .dll, .doc, .docx, docm, and .rtf and PDF) and archives containing any of the file types listed above (including ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, 7Z, Microsoft Cabinet)
	Aggressive behavioral, network, and memory analysis
	Suspicious files subjected to threat intelligence analysis in parallel with full sandbox analysis
	Detects sandbox evasion behavior
	Machine Learning technology with Deep Learning scans all dropped executable files
	Includes exploit prevention and Cryptoguard Protection technology from endpoint security
	In-depth malicious file reports and dashboard file release capability
	Optional data center selection and flexible user and group policy options on file type, exclusions, and actions on analysis
	Supports one-time download links
Logging and Reporting	
	Firewall reporting is included at no extra charge but individual log, report, and widget availability may be dependent on the respective protection module license.
	On-box reports with custom report options: Dashboards (Traffic, Security, and User Threat Quotient), Applications (App Risk, Blocked Apps, Synchronized Apps, Search Engines, Web Servers, Web Keyword Match, FTP), Network and Threats (IPS, ATP, Wireless, Security Heartbeat, Sandstorm), VPN, Email, Compliance (HIPAA, GLBA, SOX, FISMA, PCI, NERC CIP v3, CIPA)
	Current Activity Monitoring: system health, live users, IPsec connections, remote users, live connections, wireless clients, quarantine, and DoS attacks
	Report anonymization

	Report scheduling to multiple recipients by report group with flexible frequency options
	Export reports as HTML, PDF, Excel (XLS)
	Report bookmarks
	Log retention customization by category
	Full featured log viewer with column view and detailed view with powerful filter and search options, hyperlinked rule ID, and data view customization
Others	
	SSL Inspection Troubleshooting
	SD-WAN Application Routing and Synchronized SD-WAN
	Sandstorm Threat Intelligence Reporting
	High Availability (HA)
	Bridge Interface
	Flow Monitoring
	VLAN Bridge Support
	Route-based VPN
	Wildcard Domain Support in WAF
	Jumbo Frame Support
	VMware Tools and Integration With VMware Site Recovery Manager (SRM)
	Secure Syslog and Logs in the Standard Syslog Format
	DHCP Relay for Dynamic Routing
	Improved Synchronized Application Control Verdict
	Interface Renaming
	Provide an immediate Return Merchandize Authorization (RMA) or backup unit at any time the device is not working or under repair.
	Free Security Updates & Patches within the subscription period
	The Supplier should be Platinum Partner and an authorized MSP for the product.
	The Supplier should have certified engineers for the product
	Free Remote Consultation from OEM's Senior Technical Support Engineer (Minimum 3 hrs) during installation & configuration
	The Supplier must be able to provide a comprehensive after-sales support and maintenance agreement with options of 8x5 SLA
	24 X 7 Enhanced Plus Support via telephone and Email
	The Supplier of the solution must be able to provide support through Phone, text, email or other online electronic means, Web-Remote assistance and On-Site/On-call Support
	The Supplier of the solution must be able to provide quarterly systems check-up for health monitoring
	In case of hardware replacement for unsupported software: Two (2) years on parts and labor from the date of delivery
	Certification that the supplier shall issue a Warranty Certificate of the proposed solutions
	Includes 2 License/Unit for remote/branch secure access to central location for appliance based remote client:
	Maximum Throughput: 850 Mbps
	LAN Interfaces: 4 x 10/100/1000 Base-TX (1 GbE Copper)
	WAN Interfaces: 2 x 10/100/1000 Base-TX (WAN1 shared port with SFP)
	SFP Interfaces: 1x SFP Fiber (shared port with WAN1)
	Power-over Ethernet Ports: 2 PoE Ports (total power 30W)
	USB Ports: 2 x USB 3.0 (front and rear)
	COM Ports: 1 x Micro-USB
	Modular Bay: 1 for WiFi

	Wi-Fi Module: 802.11 a/b/g/n/ac Wave 1 (Wi-Fi 5) dual-band capable 2x2 MIMO 2 antennas
	Warranty: 5 YEARS

C. DEPLOYMENT SERVICES – Cover Product Assessment, Consultation and Recommendation for Implementation.

D. TECHNCAL SUPPORT AND WARRANTY

Quality assurance is expected from the SUPPLIER, such that any error or fault in any pre-installed mandatory software and installation tools delivered during the implementation shall be acted upon, resolved, mitigated and/or replaced accordingly at no cost to the organization. Likewise, upon final project acceptance, the SUPPLIER is required to after sales service and assurance that all installation are accurate, complete, operable, uncompromised, and error-free during the subcription period.

In case software is not compatible with the exisiting OPAPP server, SUPPLIER is expected to provide a new server free of charge with hardware warranty which includes 3-Year Parts, 3-Year labor, 1-Year Onsite support with next business day response.

Maintenance Services includes:
- Regular daily pattern updates and firmware updates within the subscription period.
- Includes 8 x 5 Technical Support Service within the subscription period.
- Support service includes (remote access assistance through web, phone, email and vpn access)
- Onsite Support Services if needed.
- Minimum of (2) hours response time for email support assistance.
- Minimum of (4) hours response time within Metro Manila for technical problems that cannot be resolve remotely.
- Hardware replacement or service unit with the same or higher model shall be provided within 4 hours should the equipment encounter hardware failure

IV. PROJECT DURATION

The project's duration shall not be more than the specified number of days in the Schedule of Activities. The Supplier is expected to follow the scheduled delivery strictly. Extending the period of delivery (45 days from Notice to Proceed) of the equipment and supplies will subject the Supplier to damages as provided under existing Philippine laws.

V. APPROVED BUDGET

The Approved Budget for the Contract (ABC) of the service subscription renewal is Nine Hundred Thousand Pesos (Php 900,000.00).

VI. PAYMENT SCHEDULE

Payment shall be made after submission of billing statement.

VII. SCHEDULE OF ACTIVITIES

Activities	Timeline	Remarks
Delivery of the Service (Installation and Set-up)	60 days after Contract Signing	The location of the delivery and installation shall be at 10th Floor, Agustin I Bldg., Emerald Ave., Ortigas Center, Pasig City
Inspection,Test, Evaluation and Acceptance	1 to 3 days	Inspection Committee,TWG and ICTD shall test and evaluate the performance and speed of service

VIII. POST-QUALIFICATION

The Post-qualification of the service to be provided will be based on the submitted proposal and other supporting documents.

IX. TESTING AND EVALUATION

The visual test, conformity with the specifications, and functionality test shall be conducted in accordance with the Bidding Documents and Terms of Reference.