



Republic of the Philippines
Department of Transportation and Communications
MARITIME INDUSTRY AUTHORITY

PURCHASE REQUEST

Office: <u>MISS</u>		PR No.: <u>2019-10-434</u>	
Division/Section: <u>IT Division</u>		SAI No.: <u>OCT 29 2019</u>	

Item No.	Unit	Item Description	Quantity	Unit Cost	Total Cost
1	pc.	Firewall / Network Security Device Performance Firewall throughput : 14 Gbps VPN throughput : 1.35 Gbps IPS throughput : 2.7 Gbps Antivirus throughput : 2.3 Gbps Concurrent connections: 8,200,000 New connections/sec : 135,000 Maximum licensed users : 100 License : 1 year Physical interfaces Storage (local quarantine/logs): integrated 120 GB SSD RAM : 8 GB Ethernet interfaces (fixed) : 6 GE copper No. of Flexi Port slots : 1 I/O ports : 2 x USB 3.0 (front) 1 x USB 2.0 (rear), 1 x COM (RJ45) (front) 1 x VGA (rear) Display : Multi-function LCD module	1	P345,000.00	P 345,000.00
TOTAL					P345,000.00

Signature:	 <u>Nenita S. Atienza 10/29/19</u>
Printed Name:	NENITA S. ATIENZA
Designation:	Director, MISS
Purpose:	Firewall, Web and Application Protection of MARINA

CERTIFICATION	
<input checked="" type="checkbox"/> FUNDS AVAILABLE <input type="checkbox"/> NO FUNDS AVAILABLE	 RALPH A. NARVAEZ OIC, Budget Division

<input type="checkbox"/> Approved	<input type="checkbox"/> Disapproved
PR Approver	
Signature:	
Printed Name:	VADM NARCISO A VINGSON JR
Designation:	OIC, Office of the Administrator

Note: Please indicate specific purpose other than "for official use of the Office." (e.g. monthly regular supplies, as per APP, special projects, etc.)

TERMS OF REFERENCE

SUPPLY AND DELIVERY OF A FIREWALL / NETWORK SECURITY DEVICE FOR THE MANAGEMENT INFORMATION SYSTEMS SERVICE (MISS)-MARINA CENTRAL OFFICE

I. Background

The Maritime Industry Authority (MARINA) is a government agency established pursuant to Presidential Decree No. 474 and attached to the Department of Transportation (DOTr). In compliance with Republic Act. No. 9184 known as the "Government Procurement Reform Act", the MARINA will be conducting a small value procurement for the Supply and Delivery of a firewall/network security device for the Management Information Systems Service (MISS)-MARINA Central Office.

II. Objectives

1. To procure a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.
2. To have a barrier between secured and controlled internal networks that can be trusted and untrusted outside networks, such as the Internet.

III. Approved Budget

The Approved Budget is Three Hundred Forty Five Thousand Pesos (PhP 345,000.00), inclusive of VAT and other applicable government taxes to be charged against the 2019 GAA.

IV. Deliverables

One (1) Firewall / Network Security Device

V. Technical Specifications

Hardware
Processor : Multi-core Processing Technology - Intel Xeon Dual Core G1820 @ 2.7Ghz
Form Factor : 1U Rackmount (Sliding Rails Incl.)
Memory : 8 Gb DDR3
Storage : 120 GB SSD (RAID-1)
Ethernet Ports : 6 x 1GbE built-in Copper Ports with Extra Module Slots for Copper, SFP & 10GbE SFP+
I/O Ports : 3x USB 3.0, 1x COM (RJ45), 1x VGA
Display : Multi-Function LCD module
Power Supply : Internal Auto-Ranging 110-240VAC, 50-60Hz Hot Swap Redundant, PSU optional

mutyu 10/29/19

Product Certifications (Safety, EMC) : CB, CE, FCC Class A, CTick, IC, VCCI, RCM, UL, CCC
Security Performance
Firewall Throughput : 14,000 Mbps
IPS throughput : 2,700 Mbps
VPN throughput : 1,350 Mbps
Antivirus throughput (proxy) : 2,300 Mbps
Concurrent connections : 8,200,000
New connections/sec : 135,000
Maximum licensed users : 100
General Management
Rich graphical interactive control center with traffic-light style indicators for important alerts
2-clicks-to-anywhere navigation
Advanced trouble-shooting tools in GUI (e.g. Packet Capture)
High Availability (HA) support clustering 2 devices in active-active or active-passive mode.
HA Support for dynamic addresses on WAN interfaces
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 management support from on-premise or cloud-based firewall manager
Backup and restore configurations: locally, via FTP or email; on-demand, daily, weekly or monthly
API for 3rd party integration
Secure remote access option for principal's support
Cloud-based license management
Deployment options support for hardware appliances, software, virtual, and Microsoft Azure
Firewall, Networking, and Routing
Stateful deep packet inspection firewall
FastPath Packet Optimization
User, network, or business application based firewall rules
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
Flood protection: DoS, DDoS and portscan blocking
Country blocking by geo-IP with simple country and continent selections

mitze 10/29/19

Routing: static, multicast (PIM-SM) and dynamic (RIP, BGP, OSPF)
Per-rule and policy based routing by source, destination, user/group or layer-4 service
Upstream proxy support
Protocol independent multicast routing with IGMP snooping
Bridging with STP support and ARP broadcast forwarding
VLAN DHCP support and tagging
Simultaneous DHCP Server and Relay support
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 support with tunnelling support including 6in4, 6to4, 4in6, and IPv6 rapid deployment (6rd) through IPSec
Base Traffic Shaping & Quotas
Flexible network or user based traffic shaping (QoS) (enhanced Web and App traffic shaping options)
Set user-based traffic quotas on upload/download or total traffic and cyclical or non-cyclical
Real-time VoIP optimization
Secure Wireless
Simple plug-and-play deployment of wireless access points (APs) - automatically appear on the firewall control center
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
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
Wireless repeating and bridging meshed network mode with supported Aps
Automatic channel selection background optimization
Authentication
Transparent, proxy authentication (NTLM) or client authentication
Authentication via: Active Directory, eDirectory, RADIUS, LDAP and TACACS+
Server authentication agents for Active Directory SSO
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
Customizable Captive Portal
Two factor authentication (one-time password support) for IPSec and SSL VPN, user portal, and Webadmin

metz 10/29/19

User Self-Service Portal
Download the Authentication Client under user 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 (requires Email Protection)
Setup two-factor authentication with QR Code
User Self-Service Portal
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/Android VPN client support
SSL client for Windows & configuration download via user portal
IPSec client (must support; optional to purchase)
Authentication: Pre-Shared Key (PSK), PKI (X.509), Smartcards, Token and XAUTH
Encryption: AES (128/192/256), DES, 3DES (112/168), Blowfish, RSA (up to 2048 Bit), DH groups 1/2/5/14, MD5 and SHA-256/384/512
Intelligent split-tunneling for optimum traffic routing
NAT-traversal support
Client-monitor for graphical overview of connection status
Multilingual: German, English and French
NETWORK PROTECTION FEATURES
Intrusion Prevention System (IPS)
High-performance, next-gen IPS deep packet inspection engine with selective IPS patterns for maximum performance and protection
Thousands of signatures
Support for custom IPS signatures
Flexible IPS policy deployment as part of any network or user policy with full customization
Advanced Threat Protection and Security Synchronization
Advanced Threat Protection (Detect and block zero-day attacks or network traffic attempting to contact command and control servers using multi-layered DNS, AFC, and firewall)
End-to-end security synchronization that instantly identifies compromised endpoints including the host, user, process, incident count, and time of compromise
End-to-end security synchronization that policies can limit access to network resources or completely isolate compromised systems until they are cleaned up
Clientless VPN
Unique encrypted HTML5 self-service portal with support for RDP, HTTP, HTTPS, SSH, Telnet and VNC.
Remote Ethernet Device VPN
Clientless VPN
Central Management of all RED devices
No configuration: Automatically connects through a cloud-based provisioning service
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

muty 10/19/19

Remotely de-authorize RED devices after a select period of inactivity
Compression of tunnel traffic
VLAN port configuration options
Firewall-to-Firewall RED Tunnels
WEB PROTECTION FEATURES
Web Protection and Control
Enterprise-grade web policy engine with top-down execution and inheritance with flexible user/group policy definitions and precedence, customizable activities, block/warn/allow actions, and time-of-day and day-of-week constraints
High-performance 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 policies 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
High performance web content caching
Forced caching for endpoint signature updates
File type filtering by mime-type, extension and active content types (e.g. Activex, applets, cookies, etc.)
YouTube for Schools enforcement
SafeSearch enforcement
Creative commons image search enforcement
Google Apps domain enforcement
Unscannable content handling options
Support for adding custom 3rd party URL databases
Application Protection and Control
Enhanced application control with signatures and Layer 7 patterns for thousands of applications
Dynamic application identification utilizes the end-to-end security synchronization link with the endpoint to determine apps responsible for generating unknown traffic on the network
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 Application 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 shared
LOGGING AND REPORTING FEATURES
Logs and Reports
Hundreds of on-box reports with custom report options: Dashboards (Traffic, Security, and User Threat Quotient), Applications (App Risk, Blocked Apps, Search Engines, Web Servers, FTP), Network & Threats (IPS, ATP, Wireless, Synchronized Security), VPN, Email, Compliance (HIPAA, GLBA, SOX, FISMA, PCI, NERC CIP v3, CIPA)

nutty 10/29/19

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
Full log viewer available from every screen that pops-open in a new window
Customized log viewer refresh period and color coded log lines for easy trouble-shooting
Log retention customization by category
SUPPORT FEATURES
Warranty and Support
Hardware warranty & RMA with Advanced Exchange
24x7 Enhanced Plus Support via Telephone & Email with Remote Consultation
Certified engineers for local support


VI. Delivery Schedule

1. Forty-five (45) days upon receipt of the Notice to Proceed (NTP);
2. Deliveries should be made within office hours and on regular working days;
3. MARINA shall impose penalty of 1/10 of 1% of the total value of the undelivered order for each day of delay as liquidated damages after the specified allowable number of days to deliver the units.

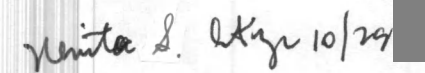
VII. Other Requirement

One (1) year warranty on parts and labor.

Prepared by:


ADRIAN G. RAMOS
 ITO-II

Approved by:


NENITA S. ATIENZA
 Director, MISS 