TERMS OF REFERENCE
FOR THE SUPPLY, DELIVERY, INSTALLATION AND TRAINING OF VARIOUS SECURITY AND NETWORK APPLIANCE

A. BACKGROUND

Weather Division experienced network problem that caused the local area network inoperable with intermittent connectivity. It took some time to find out that there was data collision. As a measure to avoid this event from happening again, Weather Division will acquire a network Analyzer and in addition to this will upgrade some of its old network switches to improve bandwidth capability.

The old network switches have already lapsed its lifetime of 5 years and its capability is limited to one gigabit only. The network switches to be acquired is capable of 10 gigabit bandwidth.

B. APPROVED BUDGET FOR THE CONTRACT (ABC)

The Approved Budget for the Contract is **Three million pesos (Php 3,000,000.00)** inclusive of VAT and all applicable government taxes.

C. PLACE AND DATE OF DELIVERY

The winning bidder shall supply and deliver the deliverables at PAGASA WFFC building within twenty (20 c.d.) calendar days from receipt of the Notice to Proceed (NTP).

D. LIST OF DELIVERABLES

1. One (1) set of Network Analytic appliance with additional portable network analyzer software including installation, configuration and deployment.
2. Five (5) sets of 24 ports Network managed switch.
3. Two (2) sets of 48 ports Network managed switch.
4. One (1) Firewall Appliance.
5. One (1) lot training; on site with meals and hands-on, total of 3 days training for five persons.

E. TECHNICAL SPECIFICATIONS

Network Monitoring and Performance Analyzer Appliance - 1 Gbps Throughput Capacity - 50,000/sec Conversation Capacity - 200,000 pps - 1 x E3 CPU, 2 TB Storage (RAID 1) - 2x8 G RAM, 4 x 1 Gbps Copper Port - 250W Power Supply - Packet Analysis Engine, directive analysis guide - Real-time dashboard - Expert diagnosis, traffic analysis, protocol analysis, process analysis, application analysis, conversation analysis, TCP transaction analysis - Detailed decoding, flexible reports, real-time alarms, dedicated security analysis - Complete 802.11 a/b/g/n support - Efficient WEP/WPA/WPA2 decryption, HTTPS decryption - Protocol customization, application customization - Task Scheduler - VoIP analysis, port analysis - Display filter, Matrix, capture filter, storage filter - Node explorer, name table, alarm, automatic trace file saving, user activity analysis - Http log, DNS log, email log, VOIP log - Email reconstruction - Replay trace files - With portable Network Analyser Software
24-Ports Manage Switch with 4 ports 10gb uplinks - 24-Port 10/100/1000Base-T - 4-Port 1G/10G Base-X SFP+ (non-combo) - AC - 1 Console Port, 264Gbps Switching Capacity, 96Mpps Packet Forwarding Rate - 4 Max. Number of 10GE Ports, 1.5MB Port Buffer, 512MB RAM - 1,000 ARP table, 16K MAC Address, 500 (IPv4/IPv6) Routing Table Size - ACL Entries : In: 1,500, Out: 500 - VLAN: 4K 802.1q VLANs, Port-based VLAN, MAC-based VLAN, Protocol-based VLAN, Private VLAN, Voice VLAN, QinQ, IP subnet-based VLAN, GVRP, Guest VLAN - Link Aggregation: AP, LACP (maximum 8 ports can be aggregated), Cross devices AP, Flow balance for link aggregation - Port Mirroring: Many-to-one mirroring, One-to-many mirroring, Flow-based mirroring, Over devices mirroring, VLAN-based mirroring, VLAN-filtering

mirroring, AP-port mirroring, RSPAN, ERSPAN
- Spanning Tree Protocols: IEEE802.1d STP, IEEE802.1w RSTP, Standard 802.1s MSTP, Port fast, BPDU filter, BPDU guard, TC guard, TC protection, ROOT guard, Spanning Tree Root Guard (STRG)
- DHCP: DHCP server, DHCP client, DHCP snooping, DHCP relay, IPv6 DHCP snooping, IPv6 DHCP client, IPv6 DHCP relay, DHCP Snooping Option 82
-64 Multiple Spanning Tree Protocol (MSTP) Instance, 128 Maximum Aggregation Port (AP)
- SDN: OpenFlow 1.0 & 1.3 SDN
-VSU (Virtual Switch Unit): Support (up to 9 stack members to ensure the effectiveness of the use, 4 members are recommended), Local and distant stacking, Cross-chassis link aggregation in the stack, Stacking via 10G Ethernet ports
- Zero Configuration: CWMP(TR069)
-Layer 2 Features: MAC, EEE, ARP, VLAN, Basic QinQ, Felix QinQ, Link aggregation, Mirroring, STP, RSTP, MSTP, Broadcast/Multicast/Unknown unicast storm control, IGMP v1/v2/v3 snooping, IPv6 MLD Snooping v1/v2, IGMP SGVL/IVGL, IGMP querier, IGMP filter, IGMP fast leave, DHCP, Jumbo frame, RLDP, LLDP, REUP, G.8032 ERPS, Layer 2 protocol tunnel
- Layer 2 Protocols: IEEE802.3, IEEE802.3u, IEEE802.3z, IEEE802.3x, IEEE802.3ad, IEEE802.1p, IEEE802.1x, IEEE802.3ab, IEEE802.1Q (GVRP), IEEE802.1d, IEEE802.1w, IEEE802.1s
- Layer 3 Features: IPv4 static routing, RIP, IPv6 static routing, RIPing
- Layer 3 Protocols (IPv4): Static routing, RIP, G.8302 Support
- ACL: Standard/Extended/Expert ACL, Extended MAC ACL, ACL 80, IPv6 ACL,
ACL logging, ACL counter, ACL remark, Global ACL, ACL redirect, Time-based ACL, Router ACL, VLAN ACL, Port-Based ACL
- QoS: 802.1p/DSCP/TOS traffic classification; Multiple queue scheduling mechanisms, such as SP, WRR, DRR, SP+WFQ, SP+WRR, SP+DRR; Input / output port-based speed limit; Port-based traffic recognition; Each port supports
8 queue priorities; flow-based rate limiting with the minimum granularity of 8Kbps, Dynamic Qos
- IPv6 ACL Support
- Reliability: VSU (virtualization technology for virtualizing multiple devices into 1); RIP GR; ERPS (G.8032); REUP dual-link fast switching technology; RLDP (Rapid Link Detection Protocol)
- Security: Binding of the IP address, MAC address, and port address; Binding of
the IPv6, MAC address, and port address; Filter illegal MAC addresses; Port-based and MAC-based 802.1x; MAB; Portal and Portal 2.0 authentication; ARP-
check; DAI; Restriction on the rate of ARP packets; Gateway anti-ARP spoofing;

Broadcast suppression; Hierarchical management by administrators and password protection; RADIUS and TACACS+; Change of Authorization; AAA security authentication (IPv4/IPv6) in device login management; SSH and SSH V2.0; BPDU guard; IP source guard; CPP, NFPP; Port protection, CoA (RADIUS change of authorization), SCP (Secure Copy) Dynamic ARP Inspection (DAI)
- Hot Patch Support
- Other Protocols: FTP, TFTP, DNS client, DNS static

48-Ports Manage Switch with 4 ports 10gb uplinks
- 48-Port 10/100/1000Base-T
- 4-Port 1G/10G Base-X SFP+ (non-combo)
- AC
-1 Console Port, 264Gbps Switching Capacity, 96Mpps Packet Forwarding Rate
- 4 Max. Number of 10GE Ports, 1.5MB Port Buffer, 512MB RAM
- 1,000 ARP table, 16K MAC Address, 500 (IPv4/IPv6) Routing Table Size
- ACL Entries : In: 1,500, Out: 500
- VLAN: 4K 802.1q VLANs, Port-based VLAN, MAC-based VLAN, Protocol-based VLAN, Private VLAN, Voice VLAN, QinQ, IP subnet-based VLAN, GVRP, Guest VLAN
- Link Aggregation: AP, LACP (maximum 8 ports can be aggregated), Cross devices AP, Flow balance for link aggregation
- Port Mirroring: Many-to-one mirroring, One-to-many mirroring, Flow-based mirroring, Over devices mirroring, VLAN-based mirroring, VLAN-filtering mirroring, AP-port mirroring, RSPAN, ERSPAN
- Spanning Tree Protocols: IEEE802.1d STP, IEEE802.1w RSTP, Standard 802.1s MSTP, Port fast, BPDU filter, BPDU guard, TC guard, TC protection, ROOT guard, Spanning Tree Root Guard (STRG)
- DHCP: DHCP server, DHCP client, DHCP snooping, DHCP relay, IPv6 DHCP snooping, IPv6 DHCP client, IPv6 DHCP relay, DHCP Snooping Option 82
-64 Multiple Spanning Tree Protocol (MSTP) Instance, 128 Maximum Aggregation Port (AP)
- SDN: OpenFlow 1.0 & 1.3 SDN
- VSU (Virtual Switch Unit): Support (up to 9 stack members to ensure the effectiveness of the use, 4 members are recommended), Local and distant stacking, Cross-chassis link aggregation in the stack, Stacking via 10G Ethernet ports
- Zero Configuration: CWMP(TR069)
- Layer 2 Features: MAC, EEE, ARP, VLAN, Basic QinQ, Felix QinQ, Link aggregation, Mirroring, STP, RSTP, MSTP, Broadcast/Multicast/Unknown unicast storm control, IGMP v1/v2/v3 snooping, IPv6 MLD Snooping v1/v2, IGMP SGVL/IVGL, IGMP querier, IGMP filter, IGMP fast leave, DHCP, Jumbo frame, RLDP, LLDP, REUP, G.8032 ERPS, Layer 2 protocol tunnel

- Layer 2 Protocols: IEEE802.3, IEEE802.3u, IEEE802.3z, IEEE802.3x, IEEE802.3ad, IEEE802.1p, IEEE802.1x, IEEE802.3ab, IEEE802.1Q (GVRP), IEEE802.1d, IEEE802.1w, IEEE802.1s - Layer 3 Features: IPv4 static routing, RIP, IPv6 static routing, RIPing - Layer 3 Protocols (IPv4): Static routing, RIP, G.8302 Support - ACL: Standard/Extended/Expert ACL, Extended MAC ACL, ACL 80, IPv6 ACL, ACL logging, ACL counter, ACL remark, Global ACL, ACL redirect, Time-based ACL, Router ACL, VLAN ACL, Port-Based ACL - QoS: 802.1p/DSCP/TOS traffic classification; Multiple queue scheduling mechanisms, such as SP, WRR, DRR, SP+WFQ, SP+WRR, SP+DRR; Input / output port-based speed limit; Port-based traffic recognition; Each port supports 8 queue priorities; flow-based rate limiting with the minimum granularity of 8Kbps, Dynamic Qos - IPv6 ACL Support - Reliability: VSU (virtualization technology for virtualizing multiple devices into 1); RIP GR; ERPS (G.8032); REUP dual-link fast switching technology; RLDP (Rapid Link Detection Protocol) - Security: Binding of the IP address, MAC address, and port address; Binding of the IPv6, MAC address, and port address; Filter illegal MAC addresses; Port-based and MAC-based 802.1x; MAB; Portal and Portal 2.0 authentication; ARP-check; DAI; Restriction on the rate of ARP packets; Gateway anti-ARP spoofing; Broadcast suppression; Hierarchical management by administrators and password protection; RADIUS and TACACS+; Change of Authorization; AAA security authentication (IPv4/IPv6) in device login management; SSH and SSH V2.0; BPDU guard; IP source guard; CPP, NFPP; Port protection, CoA (RADIUS change of authorization), SCP (Secure Copy) Dynamic ARP Inspection (DAI) - Hot Patch Support - Other Protocols: FTP, TFTP, DNS client, DNS static
Appliance with Full Guard - Intel Core i5 Quad Core 6500 @ 3.2 GHz - Form Factor: 1U rackmount - Memory: 12 GB - HDD Storage :180 GB SSD -2 10 GE SFP+ port GE copper - FLEXI PORT MODULES (OPTIONAL)* 8 port GE copper 8 port GE SFP

2 port 10 GE SFP+
4 port 10 GE SFP+
4 port GE copper
LAN bypass
4 port GE PoE
8 port GE PoE
-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
- Power Supply: Internal auto-ranging
110 - 240VAC, 50-60 Hz
Redundant PSU optional (external)
- Firewall Throughput: Minimum 30 Gbps
- IPS throughput: Minimum 8.5 Gbps
- VPN throughput: Minimum 3.2 Gbps
- Antivirus throughput (proxy): Minimum 6 Gbps
- Concurrent connections: Min. 17,500,000
- New connections/sec: Min. 200,000
- Maximum licensed users: Unrestricted
- High Availability (HA) support clustering two devices in active-active or active-passive mode Advanced trouble-shooting tools in GUI (e.g. Packet Capture)
- 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
- Backup and restore configurations: locally, via FTP or email; on-demand, daily, weekly or monthly
- API for 3rd party integration
- Remote access support from OEM directly

Firewall, Networking & Routing:

- Stateful deep packet inspection firewall
- User, group, time, or network based policies
- Access time polices per user/group
- Default Interfaces LAN, WAN, DMZ, LOCAL, VPN and WiFi
- Customizable Interfaces on LAN or DMZ
- Customizable NAT policies with IP masquerading
- Flood protection: DoS, DDoS and portscan blocking
- Country blocking by Geo-IP

- Routing: static, multicast (PIM-SM) and dynamic (BGP, OSPF
- Upstream proxy support
- Protocol independent multicast routing with IGMP snooping
- Bridging with STP support and ARP broadcast forwarding
- WAN link balancing: multiple Internet connections, auto-link health check, automatic failover, automatic and weighted balancing and granular multipath rule
- Wireless WAN support
- 802.3ad interface link aggregation
- Full configuration of DNS, DHCP and NTP
- Dynamic DNS
- IPv6 tunnelling support including 6in4, 6to4, 4in6, and IPv6 rapid deployment (6rd) through IPSec
- VLAN DHCP support and tagging
- Multiple bridge support

Wireless Protection & Control:

- Simple plug-and-play deployment of wireless access points (APs) – automatically appear on the firewall control center (no additional hardware required)
- 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
- Support for HTTPS login

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 OSX, 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-Service 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 (with 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
- SSL client for Windows & configuration download via User portal
- IPSec Client Options
- 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

Intrusion Prevention Systems (IPS)

- High-performance, next-gen IPS deep packet inspection engine with selective IPS patterns for maximum performance and protection

Advance Threat Protection

- Advanced Threat Protection (Detect and block network traffic attempting to contact command and control servers using multi-layered DNS, AFC, and firewall)

Auto VPN Connectivity

- Central Management of Auto (plug and play) VPN Device
- No configuration necessary: 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
- Remotely de-authorize VPN devices after a select period of inactivity
- Compression of tunnel traffic
- VLAN port configuration options

Clientless VPN

- Unique encrypted HTML5 self-service portal with support for RDP, HTTP, HTTPS, SSH, Telnet and VNC

Web Protection and Control

- Fully transparent Proxy for Anti-Malware and Web-filtering

- Enhanced Advanced Threat Protection (ATP)
- URL Filter database with millions of sites across 92 categories backed by OEM Security 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/ HTTPS, 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 (Dual AV)
- Real-time or batch mode scanning
- Pharming Protection
- HTTP and HTTPS scanning on a per user or network policy basis with customizable rules and exceptions
- SSL protocol tunneling detection and enforcement
- Certificate validation
- High performance web content caching
- Forced caching for Endpoint Security updates
- File type filtering by mime-type, extension and active content types (e.g. ActiveX, applets, cookies, etc.)
- YouTube for Schools enforcement/policy
- Safe Search enforcement/policy

Application Protection and Control

- Signature-based application control with patterns for thousands of applications
- 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 & App Traffic Shaping

- Custom traffic shaping (QoS) options by web category or application to limit or guarantee upload/download or total traffic priority and bitrate individually or shared

Email Protection and Control

- E-mail scanning with SMTP, POP3, and IMAP support
- Reputation service with spam outbreak monitoring based on patented Recurrent-Pattern-Detection technology
- Block spam and malware during the SMTP transaction
- Second independent malware detection engine for dual-scanning (Dual AV)
- Live Protection real-time in-the-cloud lookups for the latest threat intelligence
- Automatic signature and pattern updates
- 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
- TLS Encryption support for SMTP, POP and IMAP

- Append signature automatically to all outbound messages

Email Quarantine Management

- Spam quarantine digest and notifications options
- Malware and spam quarantines with search and filter options by date, sender, recipient, subject, and reason with option to release and delete messages
- Self-service user portal for viewing and releasing quarantined messages

Email Encryption and DLP

-SPX email encryption for one-way message encryption
- Recipient self-registration SPX password management
- Add attachments to SPX secure replies
- Completely transparent, no additional software or client required
- DLP engine with automatic scanning of emails and attachments for sensitive data
- Pre-packaged sensitive data type content control lists (CCLs) for PII, PCI, HIPAA, and more, maintained by OEMLabs

Logging and Reporting

- Built-in on-box reports with customized reporting
- Dashboards on Traffic, Security, and User Threat Quotient
- Applications Report on App Risk, Blocked Apps, Web Uses, Search Engines, Web Servers, FTP
- Network & Threats Report on IPS, ATP, Wireless
- VPN Reports
- Email usage and protection Reports
- Compliance reports i.e., HIPAA, GLBA, SOX, FISMA, NERC CIPv3, and 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
- Full log viewer with retention customization by category

F. MAINTENANCE SERVICE WARRANTY

During the 3-year subscription period, the winning bidder shall provide maintenance service warranty which shall include the following:

1) Warranty period starts from the date of acceptance.
2) Regular daily pattern updates and firmware updates within the subscription period.
3) Availability of Technical Support services via telephone, text, and email which include Remote Access Assistance thru Internet web or VPN access.

All prospective bidders shall submit their proposed Service Level Agreement (SLA).