ILOILO SCIENCE AND TECHNOLOGY UNIVERSITY
BIDS AND AWARD COMMITTEE
For Goods Offered from within the Philippines

Project Reference No. ISAT U GOODS 2026-01-001

Procurement of Firewall-(EPA)

Name of Bidder:_____

1			2		3	4	5	6	7	8
Item No.	Category	Description	Unit	Brand	Country of Origin	Quantity	Unit Price	VAT 12%	Unit Price w/Tax	Total Price w/Tax
	LOT 1	**Next Generation Firewall Appliance**								
1	Firewall	**Next Generation Firewall Appliance** Performance: 2.6 Gbps IPS throughput 1.6 Gbps NGFW throughput 1 Gbps Threat Protection throughput 20/18/10 Gbps IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP) 4.97 µs Firewall Latency (64 byte, UDP) 15 Mpps Firewall Throughput (Packet per sec) 1.5 Million Concurrent Sessions (TCP) 56,000 New Sessions/second (TCP) 10,0000 Firewall Policies 11.5 Gbps IPsec VPN Throughput (512 byte) 2000 Gateway-Gateway IPsec VPN Tunnels 16,000 Client-Gatewal IPsec VPN Tunnels 1 Gbps SSL-VPN Throughput 500 Concurrent SSL-VPN users 1 Gbps SSL Inspection Throughput Connectivity: 12 × GE RJ45 ports 4 × GE SFP slots 2 × 10GE SFP+ slots 2 × RJ45 HA ports & MGMT,USB,Console port 1U rackmount form factor Redundant Power Supply (For Leon and Barotac Nuevo Campuses Deployment)	unit			2				
2	Firewall	**Next-Generation Firewall Appliance** Performance: 5.3 Gbps IPS throughput 3.1Gbps NGFW throughput 2.8 Gbps Threat Protection throughput 39/39/28 Gbps IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP) 3.17 µs Firewall Latency (64 byte, UDP) 42 Mpps Firewall Throughput (Packet per sec) 3 Million Concurrent Sessions (TCP) 140,000 New Sessions/second (TCP) 10,0000 Firewall Policies 35 Gbps IPsec VPN Throughput (512 byte) 2000 Gateway-Gateway IPsec VPN Tunnels 16,000 Client-Gatewal IPsec VPN Tunnels 1.5 Gbps SSL-VPN Throughput 500 Concurrent SSL-VPN users 3 Gbps SSL Inspection Throughput 1 x 480 GB SSD Internal Storage Connectivity: 16 × GE RJ45 ports 8 × SFP ports 4 × 10GE SFP+ slots 2 × RJ45 HA/Management ports, USB, Console port 1U rackmount form factor Redundant Power Supply (For Miagao Campus Deployment)	unit			1				
		For both types of firewall, the subscriptions includes: (1 year subscription) 1. Intrusion Prevention System 2. Anti-Malware Protection (AV, Botnet Domains, Mobile Malware, Virus Outbreak Protection, Content Disarm and Reconstruct 3,AI-based Heuristic AV, Cloud Sandbox) 3. URL, DNS and Video Filtering 4. Anti-Spam 5. Application Control 6. Integrated SD-WAN, ZTNA, and Security Fabric Support Scope of Works *Delivery of three (3) unit NGFW) appliances installation, configuration, and integration into the existing network infrastructure. *Testing and commissioning of the firewall solution. *Conduct of knowledge transfer and basic training for technical staff. *Provision of project documentation (hard/soft copy). Supplier Certifications And Qualifications *Service center within the locality *The bidder must have at least one team member certified in a globally recognized network security program for the product offered. *The bidder must have at least one team member certified by an internationally recognized cybersec organization. Warranty And Technical Support One (1) year warranty on service One (1) year license subscription Payment Term One-time payment (After Testing and Commissioning) Delivery Period: 45 days Warranty Period: 1 year on parts/services Includes 1 year subscription After Sales Services: Service center within the locality								

	LOT 2	Next Generation Firewall with Unified Threat Management								
1	Firewall	**Next Generation Firewall with Unified Threat Management** Performance: Firewall Throughput: 80 Gbps Firewall IMIX Throughput: 37 Gbps Next-Gen Firewall (NGFW) Throughput: 30 Gbps Threat Protection Throughput: 31 Gbps IPS Throughput: 35.7 Gbps TLS/SSL Inspection Throughput: 10.6 Gbps IPsec VPN Throughput: 75 Gbps Latency (64-byte UDP): 4 µs (microsecond) Concurrent Connections: 17,200,000 New Connections per Second: 450,000 Form Factor: 1U rackmount Connectivity and Interfaces Fixed Ethernet Interfaces: 4 x GbE copper ports (with 2 bypass pairs) 4 x 2.5 GbE copper ports 4 x SFP+ 10 GbE fiber ports Flexi Port Slots: 2 bays for optional add-on modules to expand port density. Management Interfaces: 1 x RJ45 MGMT port 1 x COM RJ45 port 1 x COM Micro-USB port 2 x USB 3.0 (front) Have at least eight (4) 10Gbe Fiber Transceiver Short Range Have at least two (2) expansion slots Have at least 240 GB of storage Have hot-swappable redundant power supply Have dedicated management port Firewall Management, Networking, Routing Shall include Application Programming Interface (API) to enable integration with 3rd-party systems Support cloud-based license management Incorporate high-performance, unified Deep Packet Inspection (DPI) engine capable of performing stream-based scanning for intrusion prevention, antivirus, web filtering, application control, and TLS inspection. Customizable Network Address Translation (NAT) policies, including IP masquerading Robust flood protection mechanisms to mitigate Denial-of-Service (DoS), Distributed Denial-of-Service (DDoS), and port scan attacks. Routing protocols: Static routing, multicast routing, (PIM-SM), RIP, BGP, OSPFv3(IPv6), BGPv6. Flexible traffic shaping(Quality of Service QOS) Network Protection Intrusion Prevention System (IPS) Creation of custom IPS signatures Incorporate new IPS patterns VPN Support and Portals Support site-to-site VPN connectivity using both SSL and IPSec protocols Support 256-bit AES and 3DES, IKEv2 Perfect Forward Secrecy (PFS), RSA, X.509 certs Support route-based VPNs with traffic selectors Provide users to download SSL remote access clients for Windows OS. Email Protection Support SMTP, POP and IMAP Support reputation service with spam outbreak monitoring based on Recurrent-Pattern-Detection Block spam & malware during transaction Detect phishing URLs within emails Application Visibility and Control Offer signature-based application control Application control capabilities including: based on application categories, application characteristics, technologies used by the application, Web Server Protection Must be able to harden the web serversReverse Proxy technology URL hardening engine Support Form Hardening, SQL injection protection, cross-site scripting protection, HTTPS (TLS/SSL) encryption offloading, cookie signing with digital signature, reverse authentication, virtual server, wildcard for server paths and domains, allow/block IP ranges DNS Security Cloud-based DNS Service to enhance web security Capable of blocking access to unsafe and unwanted domains across all ports, protocols, and applications, protecting both managed & unmanaged devices Continously updated by a dedicated threat intelligence team using advanced analysis techniques to identify and block malicious & unwanted sites Updates should be applied in real-time as soon as new threats are discovered. Zero Day Protection Includes zero-day threat protection service, backed by a leading threat intelligence and analysis platform Leverage advanced static and dynamic file analysis techniques, powered by AI	unit			1				

		Capable of analyzing file types such as exe, com, dll, doc, docx, docm, rtf, pdf, zip, bzip, gzip, rar, tar, lha/lzh, 7z, and MS cabinet Provides detailed threat intelligence reports SD-WAN Supports multiple WAN link Supports application routing over preferred links via firewall rules or policy-based routing Support VPN including IPSec and SSLVPN URL Filtering Enterprise-grade URL filtering capabilities Flexible web protection deployment options, transparent proxy and explicit proxy mode inspection Comprehensive URL filtering database, containing millions of categorized websites Capable of surfing quotas, access time policies, comprehensive malware scanning, advanced malware protection, real-time threat intelligence, dual malware scanning engine, SSL inspection certificate validation, web content caching Authentication Support Active Directory, eDirectory, RADIUS, LDAP, and TACACS+ Support single sign-on (SSO) integration with AD, eDirectory, and RADIUS accounting. Support browser-based SSO authentication using transparent authentication, proxy authentication (NTLM), and Kerberos Provide authentication services for the following VPN protocols: IPsec, SSL, L2TP, PPTP. Scope of Works Delivery of (1) one firewall and all its components Assist in the project design Installation and configuration of all system component Testing and Final implementation of the proposed solution Knowledge transfer Provide project documentation Supplier Certifications And Qualifications Supplier must have a local store/office (within the locality) Authorized Distributor/Dealer/Reseller certificate from the manufacturer Manufacturer's certificate of Gold/Platinum/Tier 1 Partner Locally-based, full-time employee of the prospective bidder with proof of certificate: a. Two (2) Certified Architects b. Two (2) Senior Certified Project Manager									
		Warranty And Technical Support One (1) year warranty on service One (1) year license subscription Firmware updates during the subscription period, 24/7 via phone, web portal, and remote assistance Onsite support, if necessary Payment Term One-time payment (After activation of license) Installation and configuration of all system component Trade-up: To replace the existing firewall as it is approaching end-of-life Delivery Period: 45 days Warranty Period: 1 year on parts/services Includes 1 year subscription of the following: Xstream Protection Webserver Protection Email Protection After Sales Services: With After Sales Support / Knowledge Transfer									

Legal Capacity: _____

Signature : _____

Duty authorized to sign the Bid for and behalf of: _____