Republic of the Philippines

Tourism Infrastructure & Enterprise Zone Authority

Supply, Delivery, and Installation of Hardware and Software Firewall

TERMS OF REFERENCE

Technical Specifications	
Model : XGS 4500	
Country of Origin : USA/UK/EU	
Hardware Specifications	
Performance	
1.	Firewall throughput 80,000 Mbps
2.	Firewall IMIX 37,000 Mbps
3.	Firewall Latency (64 byte UDP) 4 µs
4.	IPS throughput 35,690 Mbps
5.	Threat Protection throughput 8,390 Mbps
6.	Concurrent Connections 17,200,000
7.	New connections/sec 450,000
8.	IPsec VPN throughput 62,000 Mbps
9.	Xstream SSL/TLS Inspection 10,600 Mbps
10.	Xstream SSL/TLSConcurrent connections 276,480
Physical interfaces	
1.	Storage(local quarantine/logs) 2 x min. 240 GB SATA-III SSD (SW RAID-1)
2.	Ethernet interfaces (fixed) 4 x GbE copper, 4 x 2.5 GbE copper, 4 x SFP+ 10 GbE fiber
3.	Bypass port pairs: 2
4.	Management ports 1 x RJ45 MGMT, 1 x COM RJ45 1 x Micro-USB (cable incl.)
5.	Other I/O ports 2 x USB 3.0 (front)
6.	Number of expansion slots 2
7.	Max. total port density : 28
8.	Max. Power-over-Ethernet : 2 modules: 4 ports, 60W max. each
Physical specifications	
1.	Mounting:1U rackmount (sliding rails incl.)
2.	Dimensions Width x Height x Depth 438 x 44 x 510 mm
3.	Weight 9.7 kg/21.38 lbs (unpacked), 15.9 kg/35.05 lbs (packed)
Environment	
1.	Power supply : Internal Hot Swappable auto-ranging AC-DC 100-240VAC 100-240VAC, 3.7-7.4A@50-60 Hz External Redundant PSU Option
2.	Power consumption : 151 W/515.74 BTU/hr (idle), 268.35 W/916.56 BTU/hr (max.)
3.	Operating temperature 0°C to 40°C (operating) -20 to +70°C (storage)
4.	Humidity 10% to 90%, non-condensing
Product Certifications	
1.	Certifications CB, CE, UL, FCC, ISED, VCCI, CCC, KC, BSMI, NOM, Anatel

Base Firewall Features	
General Management	
1.	Purpose-built, streamlined user interface and firewall rule management for large rule sets with grouping with at-a-glance rule feature and enforcement indicators
2.	Two-factor authentication (One-time-password) support for administrator access, user portal, IPSec and SSL VPN
3.	Advanced trouble-shooting tools in GUI (e.g. Packet Capture)
4.	High Availability (HA) support clustering two devices in active-active or active-passive mode with plug-and-play Quick HA setup
5.	HA support in AWS using the AWS Transit Gateway
6.	Full command-line-interface (CLI) accessible from GUI
7.	Role-based administration
8.	Automated firmware update notification with easy automated update process and roll-back features
9.	Reusable system object definitions for networks, services, hosts, time periods, users and groups, clients and servers
10.	Self-service user portal
11.	Configuration change tracking
12.	Flexible device access control for services by zones
13.	Email or SNMP trap notification options
14.	SNMPv3 and Netflow support
15.	Central management support via Cloud-based Unified Console
16.	Automatic Email Notifications for any important event
17.	Backup and restore configurations: locally, via FTP or email; on-demand, daily, weekly or monthly
18.	API for 3rd party integration
19.	Interface renaming
20.	Remote access option for Sophos Support
21.	Cloud-based license management via Licensing Portal
22.	Syslog support
23.	Real-Time Flow Monitoring
24.	Traffic light style indicators
25.	Instant Insights At a Glance
26.	Quick Drill-down Interaction with Any Control Center Widget
27.	SNMP with a Custom MIB and support for IPSec VPN Tunnels
28.	Support for new AWS instances (C5/M5 and T3)
29.	Support for cloud formation templates
30.	Virtual WAN zone support on custom gateways for post deployment single arm usage
31.	Supports a broad range of virtualization platforms and can also be deployed as a software appliance on your own x86 Intel hardware
32.	Available in the AWS marketplace with a pay-as-you-go (PAYG) license model, or bring your own license (BYOL) to best fit your needs.
33.	Certified and optimized for Azure and is available in the Microsoft Azure Marketplace. Can take a free test drive or the flexible PAYG or BYOL licensing options.

Base Firewall Features	
General Management	
34.	Certified and optimized for Azure and is available in the Microsoft Azure Marketplace. Can take a free test drive or the flexible PAYG or BYOL licensing options.
35.	Nutanix AHV and Nutanix Flow support
36.	Stronger password hash algorithm (requires a password change)
Central Firewall Management	
1.	Cloud-based management and reporting for multiple firewalls provides group policy management and a single console for all your Sophos IT security products
2.	Group policy management allows objects, settings, and policies to be modified once and automatically synchronized to all firewalls in the group
3.	Task Manager provides a full historical audit trail and status monitoring of group policy changes
4.	Backup firmware management which stores the last five configuration backup files for each firewall with one that can be pinned for permanent storage and easy access
5.	Firmware updates which offer one-click firmware updates to be applied to any device
6.	Zero-touch deployment enables the initial configuration to be performed in Cloud-based management and then exported for loading onto the device from a flash drive at startup, automatically connecting the device back to Sophos Central
7.	Group firewall management via the Partner Dashboard
8.	Firmware update scheduling
9.	Multi-firewall reporting across firewall groups
10.	Save, schedule and export reports from Sophos Central
Firewall, Networking & Routing	
1.	Stateful deep packet inspection firewall
2.	Packet processing architecture that provides extreme levels of visibility, protection, and performance through stream-based packet processing
3.	TLS inspection with high performance, support for TLS 1.3 with no downgrading, port agnostic, enterprise-grade polices, unique dashboard visibility, and compatibility troubleshooting
4.	DPI Engine that provides stream scanning protection for IPS, AV, Web, App Control, and TLS Inspection in a single high-performance engine
5.	Accelerates SaaS, SD-WAN, and cloud traffic such as VoIP, video, and other trusted applications via FastPath through the new Xstream Flow Processors.
6.	Network Flow FastPath delivers policy-driven and intelligent acceleration of trusted traffic automatically
7.	Improved FastPath support for active-passive pairs

Base Firewall Features	
Firewall, Networking & Routing	
8.	Pre-packaged exception list
9.	Covers all ports/protocols
10.	Supports all modern cypher suites
11.	Unmatched visibility and error handing
12.	User, group, time, or network based policies
13.	Access time polices per user/group
14.	Enforce policy across zones, networks, or by service type
15.	Zone-based firewall
16.	Default zones for LAN, WAN, DMZ, LOCAL, VPN and WiFi
17.	Full VLAN support
18.	Zone and VLAN isolation and zone-based policy support.
19.	Micro-segmentation and auto-isolation via Synchronized Security
20.	Custom zones on LAN or DMZ
21.	Customizable NAT policies with IP masquerading and full object support to redirect or forward multiple services in a single rule with a convenient NAT rule wizard to quickly and easily create complex NAT rules in just a few clicks
22.	Flood protection: DoS, DDoS and portscan blocking
23.	Country blocking by geo-IP
24.	Advanced Routing: static, multicast (PIM-SM), and dynamic (RIP, BGP, OSPF) with full 802.1Q VLAN support
25.	Upstream proxy support
26.	Protocol independent multicast routing with IGMP snooping
27.	Bridging with STP support and ARP broadcast forwarding
28.	VLAN DHCP support and tagging
29.	VLAN bridge support
30.	Jumbo Frame Support
31.	SD-WAN link balancing: multiple Internet connections, auto-link health check, automatic failover, automatic and weighted balancing, and granular multipath rules
32.	Wireless WAN support (n/a in virtual deployments)

Base Firewall Features	
Firewall, Networking & Routing	
33.	802.3ad interface link aggregation
34.	Full configuration of DNS, DHCP and NTP
35.	Dynamic DNS (DDNS)
36.	IPv6 Ready Logo Program Approval Certification
37.	IPv6 tunnelling support including 6in4, 6to4, 4in6, and IPv6 rapid deployment (6rd) through IPSec
SD - WAN	
1.	Support for multiple WAN link options including VDSL, DSL, cable, and 3G/4G/LTE cellular with essential monitoring, balancing, failover and fail-back
2.	Application path selection and routing, which is used to ensure quality and minimize latency for mission-critical applications such as VoIP
3.	Synchronized SD-WAN, a Synchronized Security feature which leverages the added clarity and reliability of application identification that comes with the sharing of Synchronized Application Control information between managed endpoints and Firewall
4.	Synchronized SD-WAN application routing over preferred links via firewall rules or policy-based routing
5.	Affordable, flexible, and zero-touch or low-touch deployment
6.	Robust VPN support including IPSec and SSL VPN
7.	Centralized VPN orchestration
8.	Unique RED Layer 2 tunnel with routing
9.	Integration with Azure Virtual WAN for a complete SD-WAN overlay network
Base Traffic Shaping & Quotas	
1.	Flexible network or user based traffic shaping (QoS) (enhanced Web and App traffic shaping options included with the Web Protection subscription)
2.	Set user-based traffic quotas on upload/download or total traffic and cyclical or non-cyclical
3.	Real-time VoIP optimization
4.	DSCP marking

Base Firewall Features	
Secure Wireless	
5.	Simple plug-and-play deployment of Sophos wireless access points (APs) — automatically appear on the firewall control center
6.	High performance with the latest 802.11ac, Wave 2 wireless standard, and powerful radios
7.	Central monitoring and management of APs and wireless clients through the built-in wireless controller
8.	Bridge APs to LAN, VLAN, or a separate zone with client isolation options
9.	Multiple SSID support per radio including hidden SSIDs
10.	Support for the latest security and encryption standards including WPA2 Personal and Enterprise
11.	Channel width selection option
12.	Support for IEEE 802.1X (RADIUS authentication) with primary and secondary server support
13.	Support for 802.11r (fast transition)
14.	Hotspot support for (custom) vouchers, password of the day, or T&C acceptance
15.	Wireless guest Internet access with walled garden options
16.	Time-based wireless network access
17.	Wireless repeating and bridging meshed network mode with supported Aps
18.	Automatic channel selection background optimization
19.	Support for HTTPS login
20.	Rogue AP detection (available only with XG Firewall devices with integrated Wi-Fi)
Authentication	
1.	Synchronized User ID utilizes Synchronized Security to share currently logged in Active Directory user ID between Sophos endpoints and the firewall without an agent on the AD server or client
2.	Authentication via: Active Directory, eDirectory, RADIUS, LDAP and TACACS+
3.	Server authentication agents for Active Directory SSO, STAS, SATC
4.	Single sign-on: Active directory, eDirectory, RADIUS Accounting
5.	Radius Timeout with Two-Factor Authentication (2FA)
6.	Client authentication agents for Windows, Mac OS X, Linux 32/64
7.	Browser SSO authentication: Transparent, proxy authentication (NTLM) and Kerberos

Base Firewall Features	
Authentication	
8.	Browser Captive Portal
9.	Authentication certificates for iOS and Android
10.	Authentication services for IPSec, SSL, L2TP, PPTP
11.	Google Chromebook authentication support for environments with Active Directory and Google G Suite
12.	API-based authentication
13.	Azure AD integration
14.	Support for creating users with UPN format for RADIUS authentication
User Self- Serve Portal	
1.	Download the Sophos Authentication Client
2.	Download SSL remote access client (Windows) and configuration files (other OS)
3.	Hotspot access information
4.	Change user name and password
5.	View personal internet usage
6.	Access quarantined messages and manage user-based block/allow sender lists (requires Email Protection)
Base VPN Options	
1.	IPSec and SSL VPN tunnels
2.	Wizard-based orchestration
3.	Site-to-site VPN: SSL, IPSec, 256- bit AES/3DES, PFS, RSA, X.509 certificates, pre-shared key
4.	Remote Ethernet Device (RED) site-to-site VPN tunnel (robust and light-weight)
5.	L2TP and PPTP
6.	Route-based VPN
7.	Remote access: SSL, IPsec, iPhone/iPad/ Cisco/Andriod VPN client support
8.	IKEv2 Support
9.	SSL client for Windows and configuration download via user portal
10.	Enforcement of TLS 1.2 for SSL site-to-site and remote access VPN tunnels

Base Firewall Features	
Connect VPN Client	
1.	IPSec and SSL support
2.	Easy provisioning and deployment
3.	Free (unlimited SSL remote access licenses included at no extra charge)
4.	Authentication: Pre-Shared Key (PSK), PKI (X.509), Token and XAUTH
5.	Enables Synchronized Security and Security Heartbeat for remote connected users
6.	Intelligent split-tunneling for optimum traffic routing
7.	NAT-traversal support
7.	Client-monitor for graphical overview of connection status
8.	Mac and Windows Support
9.	Remote access IPSec policy provisioning with Sophos Connect v2.1
10.	Group support for Sophos Connect which enables imports from AD/LDAP etc.
Network Protection Subscription	
Intrusion Prevention (IPS)	
1.	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
2.	Zero-day threat protection
3.	Perimeter Defenses
4.	Thousands of signatures
5.	Granular category selection
6.	Support for custom IPS signatures
7.	IPS Policy Smart Filters enable dynamic policies that automatically update as new patterns are added
ATP and Security Heartbeat	
1.	Advanced Threat Protection (detect and block network traffic attempting to contact command and control servers using multi-layered DNS, AFC, and firewall)
2.	Sophos Security Heartbeat instantly identifies compromised endpoints including the host, user, process, incident count, and time of compromise
3.	Sophos Security Heartbeat policies can limit access to network resources or completely isolate compromised systems until they are cleaned

Network Protection Subscription	
ATP and Security Heartbeat	
4.	Lateral Movement Protection further isolates compromised systems by having healthy Sophos -managed endpoints reject all traffic from unhealthy endpoints preventing the movement of threats even on the same broadcast domain
5.	Intelligent firewall policies
6.	Multi-layered, call-home protection
SD – Remote Ethernet Device Management	
1.	Zero-touch deployment auto-provisioning SD-WAN edge device
2.	Central management of all SD-RED devices
3.	No configuration: Automatically connects through a cloud-based provisioning service
11.	Enterprise-grade encryption
12.	Split tunnel options
13.	Secure encrypted tunnel using digital X.509 certificates and AES 256-bit encryption
14.	Virtual Ethernet for reliable transfer of all traffic between locations
8.	IP address management with centrally defined DHCP and DNS Server configuration
9.	Remotely de-authorize RED device after a select period of inactivity
10.	Compression of tunnel traffic
11.	VLAN port configuration options
12.	Integrated wireless options
13.	Ultra affordable
Clientless VPN	
1.	Unique encrypted HTML5 self-service portal with support for RDP, HTTP, HTTPS, SSH, Telnet, and VNC

Web Protection Subscription	
Web Protection and Control	
1.	Fully transparent proxy for anti-malware and web-filtering
2.	Enhanced Advanced Threat Protection
3.	URL Filter database with millions of sites across 92 categories backed by OEMLabs
4.	Surfing quota time policies per user/group
5.	Access time polices per user/group
6.	Malware scanning: block all forms of viruses, web malware, trojans and spyware on HTTP/S, FTP and web-based email
7.	Advanced web malware protection with JavaScript emulation
8.	Live Protection real-time in-the-cloud lookups for the latest threat intelligence
9.	Second independent malware detection engine (Avira) for dual-scanning
10.	Real-time or batch mode scanning
11.	Pharming Protection
12.	HTTP and HTTPS scanning on a per user or network policy basis with customizable rules and exceptions
13.	SSL protocol tunnelling detection and enforcment
14.	Certificate validation
15.	High performance web content caching
16.	Forced caching for Sophos Endpoint updates
17.	File type filtering by mime-type, extension and active content types (e.g. Activex, applets, cookies, etc.)
18.	YouTube for Schools enforcement per policy (user/group)
19.	SafeSearch enforcement (DNS-based) for major search engines per policy (user/group)
20.	Web keyword monitoring and enforcement to log, report or block web content matching keyword lists with the option to upload customs lists
21.	Block Potentially Unwanted Applications (PUAs)
22.	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
23.	User/Group policy enforcement on Google Chromebooks
24.	Auto web-filtering of Internet Watch Foundation (IWF) identified sites containing child sexual abuse

Web Protection Subscription	
Cloud Application Visibility	
1.	Control Center widget displays amount of data uploaded and downloaded to cloud applications categorized as new, sanctioned, unsanctioned or tolerated
2.	Discover Shadow IT at a glance
3.	Drill down to obtain details on users, traffic, and data
4.	One-click access to traffic shaping policies
5.	Filter cloud application usage by category or volume
6.	Detailed customizable cloud application usage report for full historical reporting
Application Protection and Control	
1.	Synchronized App Control to automatically, identify, classify, and control all unknown Windows and Mac applications on the network by sharing information between managed endpoints and the firewall
2.	Signature-based application control with patterns for thousands of applications
3.	Cloud Application Visibility and Control to discover Shadow IT
4.	App Control Smart Filters that enable dynamic policies which automatically update as new patterns are added
5.	Micro app discovery and control
6.	Application control based on category, characteristics (e.g., bandwidth and productivity consuming), technology (e.g. P2P), and risk level
7.	Per-user or network rule application control policy enforcement
Web & App Traffic Shaping	
1.	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
Zero-Day Protection Subscription	
Dynamic Sandbox Analysis	
1.	Full integration into your security solution dashboard
2.	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)
3.	Aggressive behavioral, network, and memory analysis
4.	Detects sandbox evasion behavior

Web Protection Subscription	
Cloud Application Visibility	
7.	Control Center widget displays amount of data uploaded and downloaded to cloud applications categorized as new, sanctioned, unsanctioned or tolerated
8.	Discover Shadow IT at a glance
9.	Drill down to obtain details on users, traffic, and data
10.	One-click access to traffic shaping policies
11.	Filter cloud application usage by category or volume
12.	Detailed customizable cloud application usage report for full historical reporting
Application Protection and Control	
1.	Synchronized App Control to automatically, identify, classify, and control all unknown Windows and Mac applications on the network by sharing information between managed endpoints and the firewall
2.	Signature-based application control with patterns for thousands of applications
3.	Cloud Application Visibility and Control to discover Shadow IT
4.	App Control Smart Filters that enable dynamic policies which automatically update as new patterns are added
5.	Micro app discovery and control
6.	Application control based on category, characteristics (e.g., bandwidth and productivity consuming), technology (e.g. P2P), and risk level
7.	Per-user or network rule application control policy enforcement
Web & App Traffic Shaping	
1.	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
Zero-Day Protection Subscription	
Dynamic Sandbox Analysis	
1.	Full integration into your security solution dashboard
2.	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)
3.	Aggressive behavioral, network, and memory analysis
4.	Detects sandbox evasion behavior

Zero-Day Protection Subscription	
Dynamic Sandbox Analysis	
5.	Machine Learning technology with Deep Learning scans all dropped executable files
6.	Includes exploit prevention and Cryptoguard Protection technology from endpoint security
7.	In-depth malicious file reports and dashboard file release capability
8.	Optional data center selection and flexible user and group policy options on file type, exclusions, and actions on analysis
9.	Supports one-time download links
10.	Deep learning static file analysis
11.	Multiple Machine Learning Models
12.	Dynamic sandboxing analysis
13.	Suspicious files subjected to threat intelligence analysis in parallel with full sandbox analysis
Threat Intelligence Analysis	
1.	All files containing active code downloaded via the web or coming into the firewall as email attachments such as 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) are automatically sent for Threat Intelligence Analysis
2.	Files are checked against OEMLabs' massive threat intelligence database and subjected to multiple machine learning models to identify new and unknown malware
3.	Extensive reporting includes a dashboard widget for analyzed files, a detailed list of the files that have been analyzed and the analysis results, and a detailed report outlining the outcome of each machine learning model.
4.	Static and Dynamic files analysis
Reporting	
Central Firewall Reporting	
1.	Pre-defined reports with flexible customization options
2.	Reporting for Firewalls (hardware, software, virtual, and cloud)
3.	Intuitive user interface provides graphical representation of data
4.	Report dashboard provides an at-a-glance view of events over the past 24 hours
5.	Easily identify network activities, trends, and potential attacks
6.	Easy backup of logs with quick retrieval for audit needs

Reporting	
Central Firewall Reporting	
7.	Simplified deployment without the need for technical expertise
8.	Create custom reports with powerful visualization tools
9.	Syslog search and view
10.	Syslog data storage in Sophos Central
11.	On-demand reporting in Sophos Central
12.	7 day cloud storage for Central Firewall reporting
13.	New Cloud Application (CASB) report
14.	No extra charge
On-Box Reporting	
1.	No extra charge
2.	Hundreds of 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)
3.	Built-in storage on XGS Series for unlimited log data storage for historical reporting
4.	Current Activity Monitoring: system health, live users, IPSec connections, remote users, live connections, wireless clients, quarantine, and DoS attacks
5.	Report anonymization
6.	Report scheduling to multiple recipients by report group with flexible frequency options
7.	Export reports as HTML, PDF, Excel (XLS)
8.	Report bookmarks
9.	Log retention customization by category
10.	Syslog Support
11.	Full-featured Live Log Viewer with column view and detailed view with powerful filter and search options, hyperlinked rule ID, and data view customization
WARRANTY	
1.	1 year on license, 3 years on hardware
TRAINING	
1.	Online/Onsite training; inclusive of training materials, meals and certificate of attendance

Republic of the Philippines
Tourism Infrastructure & Enterprise Zone Authority

REQUIREMENTS

1. The Bidder must be an authorized reseller/authorized dealer of the brand being offered. **A current valid manufacturer's certification** required as part of the technical component on bid proposal.

2. The Bidder must not exceed to forty five (45) days delivery lead-time including installation and testing upon receipt of Notice to Proceed.

ESTIMATED PROJECT COST

Approved Budget for the Contract (ABC) is **TWO MILLION FOUR HUNDRED THOUSAND PESOS ONLY (P 2,400,000.00)**

Prepared by:

MARY GRACE S. MENDEZ
Supervising Data Controller

Noted by:

RAQUEL S. DELACRUZ
Manager, MISD

Approved by:

MARK T. LAPID
Chief Operating Officer