development academy of the philippines

Telefax: 631-21-42

Request for Quotation

Date:
PR #:401881

Please quote your lowest price on the item/s listed below stating the shortest time of delivery and submit/fax/email your quotation duly signed by your representative not later than _______________________________________.

THE PROJECT WILL ONLY BE AWARDED TO PLATINUM REGISTERED PHILGEPS SUPPLIERS FOR COMPETITIVE BIDDING AND TO AT LEAST RED MEMBER REGISTERED SUPPLIERS TO ALTERNATIVE MODE OF PROCUREMENT.
TO REGISTER, KINDLY CLICK THE LINK https://www.philgeps.gov.ph/Suppliers/add

QTY	UNIT	ITEM DESCRIPTION/SPECIFICATION	UNIT PRICE
1	Lot	Supply, Delivery, and Product Support for the Firewall Software Sophos XG310 License Duration: 02 September 2022 - 02 September 2023 See the succeeding pages for the terms of reference. ABC: Php 600,000.00	

NOTE:

1. **ALL ENTRIES MUST BE CLEAR AND READABLE.**
2. **DELIVERY PERIOD WITHIN 7 CALENDAR DAYS UPON PO CONFORME.**
3. **WARRANTY SHALL BE ATLEAST SIX (6) MONTHS FOR SUPPLIES & MATERIALS, ATLEAST ONE (1) YEAR FOR EQUIPMENT, FROM DATE OF ACCEPTANCE BY THE PROCURING ENTITY.(if applicable)**
4. **PRICE VALIDITY SHALL BE FOR A PERIOD OF 90 CALENDAR DAYS.**
5. **PhilGEPS REGISTRATION CERTIFICATE SHALL BE ATTACHED/FAX/EMAILED UPON SUBMISSION OF THE QUOTATION (IF EXPIRED OR DAP HAS NO FILE).**
6. **TERMS OF PAYMENT 30 DAYS AFTER DELIVERY OF ITEM/S OR FINAL ACCEPTANCE.**

I/We quote you on the item/s at prices noted above.

____
Printed Name / Signature; Date

Tel. No. / Cellphone No. : ______________________________

E-mail address: ______________________________

Name of supplier: ______________________________

Tender Specification of Sophos Firewall

Technical Specifications	
	Model :
	Country of Origin : USA/UK/EU
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 with plug-and-play Quick HA setup
	HA support in AWS using the AWS Transit Gateway
	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
	SNMPv3 and Netflow support
	Central management support via Cloud-based Unified Console
	Automatic Email Notifications for any important event
	Backup and restore configurations: locally, via FTP or email; on-demand, daily, weekly or monthly
	API for 3rd party integration
	Interface renaming
	Remote access option for Sophos Support
	Cloud-based license management via Licensing Portal

	Syslog support
	Real-Time Flow Monitoring
	Traffic light style indicators
	Instant Insights At a Glance
	Quick Drill-down Interaction with Any Control Center Widget
	SNMP with a Custom MIB and support for IPSec VPN Tunnels
	Support for new AWS instances (C5/M5 and T3)
	Support for cloud formation templates
	Virtual WAN zone support on custom gateways for post deployment single arm usage
	Supports a broad range of virtualization platforms and can also be deployed as a software appliance on your own x86 Intel hardware
	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.
	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.
	Nutanix AHV and Nutanix Flow support
	Stronger password hash algorithm (requires a password change)
	Central Firewall Management
	Cloud-based management and reporting for multiple firewalls provides group policy management and a single console for all your Sophos IT security products
	Group policy management allows objects, settings, and policies to be modified once and automatically synchronized to all firewalls in the group
	Task Manager provides a full historical audit trail and status monitoring of group policy changes
	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
	Firmware updates which offer one-click firmware updates to be applied to any device
	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
	Group firewall management via the Partner Dashboard
	Firmware update scheduling
	Multi-firewall reporting across firewall groups
	Save, schedule and export reports from Sophos Central
	Firewall, Networking & Routing

	Stateful deep packet inspection firewall
	Packet processing architecture that provides extreme levels of visibility, protection, and performance through stream-based packet processing
	TLS inspection with high performance, support for TLS 1.3 with no downgrading, port agnostic, enterprise-grade polices, unique dashboard visibility, and compatibility troubleshooting
	DPI Engine that provides stream scanning protection for IPS, AV, Web, App Control, and TLS Inspection in a single high-performance engine
	Accelerates SaaS, SD-WAN, and cloud traffic such as VoIP, video, and other trusted applications via FastPath through the new Xstream Flow Processors.
	Network Flow FastPath delivers policy-driven and intelligent acceleration of trusted traffic automatically
	Improved FastPath support for active-passive pairs
	Pre-packaged exception list
	Covers all ports/protocols
	Supports all modern cypher suites
	Unmatched visibility and error handing
	User, group, time, or network based policies
	Access time polices per user/group
	Enforce policy across zones, networks, or by service type
	Zone-based firewall
	Default zones for LAN, WAN, DMZ, LOCAL, VPN and WiFi
	Full VLAN support
	Zone and VLAN isolation and zone-based policy support.
	Micro-segmentation and auto-isolation via Synchronized Security
	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 with a convenient NAT rule wizard to quickly and easily create complex NAT rules in just a few clicks
	Flood protection: DoS, DDoS and portscan blocking
	Country blocking by geo-IP
	Advanced Routing: static, multicast (PIM-SM), and dynamic (RIP, BGP, OSPF) with full 802.1Q VLAN support
	Upstream proxy support
	Protocol independent multicast routing with IGMP snooping
	Bridging with STP support and ARP broadcast forwarding
	VLAN DHCP support and tagging
	VLAN bridge support

	Jumbo Frame Support
	SD-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 (DDNS)
	IPv6 Ready Logo Program Approval Certification
	IPv6 tunnelling support including 6in4, 6to4, 4in6, and IPv6 rapid deployment (6rd) through IPSec
	SD-WAN
	Support for multiple WAN link options including VDSL, DSL, cable, and 3G/4G/LTE cellular withessential monitoring, balancing, failover and fail-back
	Application path selection and routing, which is used to ensure quality and minimize latency for mission-critical applications such as VoIP
	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
	Synchronized SD-WAN application routing over preferred links via firewall rules or policy-based routing
	Affordable, flexible, and zero-touch or low-touch deployment
	Robust VPN support including IPSec and SSL VPN
	Centralized VPN orchestration
	Unique RED Layer 2 tunnel with routing
	Integration with Azure Virtual WAN for a complete SD-WAN overlay network
	Base Traffic Shaping & Quotas
	Flexible network or user based traffic shaping (QoS) (enhanced Web and App traffic shaping options included with the Web Protection subscription)
	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 Sophos wireless access points (APs) — automatically appear on the firewall control center
	High performance with the latest 802.11ac, Wave 2 wireless standard, and powerful radios
	Central monitoring and management of 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 standards 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)
	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
	Rogue AP detection (available only with XG Firewall devices with integrated Wi-Fi)
	ZTNA
	Sophos Firewall integrates with Sophos Zero Trust Network Access (ZTNA) to offer a secure and simple way for users to securely connect to important applications and data.
	Securely connect users to applications
	Cloud and on-premises application support
	Remote access from anywhere
	Device health integrates with Synchronized Security
	Authentication
	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
	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
	Radius Timeout with Two-Factor Authentication (2FA)
	Client authentication agents for Windows, Mac OS X, Linux 32/64
	Browser SSO authentication: Transparent, proxy authentication (NTLM) and Kerberos
	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 G Suite
API-based authentication
Azure AD integration
Support for creating users with UPN format for RADIUS authentication
User Self-Serve Portal
Download the Sophos 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
IPSec and SSL VPN tunnels
Wizard-based orchestration
Site-to-site VPN: SSL, IPSec, 256- bit AES/3DES, PFS, RSA, X.509 certificates, pre-shared key
Remote Ethernet Device (RED) site-to-site VPN tunnel (robust and light-weight)
L2TP and PPTP
Route-based VPN
Remote access: SSL, IPsec, iPhone/iPad/ Cisco/Andriod VPN client support
IKEv2 Support
SSL client for Windows and configuration download via user portal
Enforcement of TLS 1.2 for SSL site-to-site and remote access VPN tunnels
Sophos Connect VPN Client
IPSec and SSL support
Easy provisioning and deployment
Free (unlimited SSL remote access licenses included at no extra charge)
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
Remote access IPSec policy provisioning with Sophos Connect v2.1
Group support for Sophos Connect which enables imports from AD/LDAP etc.

Network Protection Subscription	
	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
	Zero-day threat protection
	Perimeter Defenses
	Thousands of signatures
	Granular category selection
	Support for custom IPS signatures
	IPS Policy Smart Filters enable dynamic policies that 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)
	Sophos Security Heartbeat instantly identifies compromised endpoints including the host, user, process, incident count, and time of compromise
	Sophos Security Heartbeat policies can limit access to network resources or completely isolate compromised systems until they are cleaned
	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
	Intelligent firewall policies
	Multi-layered, call-home protection
	SD-Remote Ethernet Device Management
	Zero-touch deployment auto-provisioning SD-WAN edge device
	Central management of all SD-RED devices
	No configuration: Automatically connects through a cloud-based provisioning service
	Enterprise-grade encryption
	Split tunnel options
	Secure encrypted tunnel using digital X.509 certificates and AES 256-bit 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 RED device after a select period of inactivity
	Compression of tunnel traffic

	VLAN port configuration options
	Integrated wireless options
	Ultra affordable
	Clientless VPN
	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 anti-malware and web-filtering
	Enhanced Advanced Threat Protection
	URL Filter database with millions of sites across 92 categories backed by OEMLabs
	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 (Avira) for dual-scanning
	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 tunnelling detection and enforcment
	Certificate validation
	High performance web content caching
	Forced caching for Sophos Endpoint updates
	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 (PUAs)
	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

	Auto web-filtering of Internet Watch Foundation (IWF) identified sites containing child sexual abuse
	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 managed 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 & 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
Zero-Day Protection Subscription	
	Dynamic Sandbox Analysis
	Full integration into your 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
	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
	Deep learning static file analysis
	Multiple Machine Learning Models
	Dynamic sandboxing analysis
	Suspicious files subjected to threat intelligence analysis in parallel with full sandbox analysis
	Threat Intelligence Analysis
	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
	Files are checked against OEMLabs' massive threat intelligence database and subjected to multiple machine learning models to identify new and unknown malware
	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.
	Static and Dynamic files analysis
Central Orchestration *Expected soon	
	SD-WAN Orchestration
	SD-WAN and VPN orchestration with easy and automated wizard-based creation of site-to-site VPN tunnels between network locations using an optimal architecture (hub-and-spoke, full mesh, or some combination). Supports IPSec, SSL or RED VPN tunnels. Integrates seamlessly with SD-WAN features for application prioritization, routing optimization, and leveraging multiple WAN links for resiliency and performance.
	Central Firewall Reporting Advanced
	30-days of cloud data storage for historical firewall reporting with advanced features to save, schedule and export custom reports.
	XDR and MTR Connector
	Ready to integrate with Sophos Extended Threat Detection and Response (XDR) for crossproduct threat hunting and analysis
	Support for Sophos 24/7 Managed Threat Response (MTR) service

Email Protection Features	**OPTIONAL SUBSCRIPTION (ADD-ON)**	
		Email Protection and Control (ADD-ON)
		Full MTA store and forward support
		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
		DKIM and BATV anti-spam protection
		Spam greylisting and Sender Policy Framework (SPF) protection
		Recipient verification for mistyped email addresses
		Second independent malware detection engine (Avira) for dual-scanning
		Live Protection real-time in-the-cloud lookups for the latest threat intelligence
		Live Anti-spam
		Automatic signature and pattern updates
		Smart host support for outbound relays
		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 with granular policy options and exceptions
		TLS Encryption support for SMTP, POP and IMAP
		Append signature automatically to all outbound messages
		Email archiver
		Individual user-based block and allow sender lists maintained through the user portal
		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-serve user portal for viewing and releasing quarantined messages
		Email Encryption and DLP
		Patent-pending SPX 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
Web Server Protection Features		

OPTIONAL SUBSCRIPTION (ADD-ON)	**Web Application Firewall Protection (ADD-ON)**
	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 (TLS/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 Application Firewall performance parameters
	Scan size limit option
	Allow/Block IP ranges
	Wildcard support for server paths and domains
	Automatically append a prefix/suffix for authentication
Reporting	
	Central Firewall Reporting
	Pre-defined reports with flexible customization options
	Reporting for Firewalls (hardware, software, virtual, and cloud)
	Intuitive user interface provides graphical representation of data
	Report dashboard provides an at-a-glance view of events over the past 24 hours
	Easily identify network activities, trends, and potential attacks
	Easy backup of logs with quick retrieval for audit needs
	Simplified deployment without the need for technical expertise
	Create custom reports with powerful visualization tools
	Syslog search and view
	Syslog data storage in Sophos Central
	On-demand reporting in Sophos Central
	7 day cloud storage for Central Firewall reporting

	New Cloud Application (CASB) report
	No extra charge
	Central Firewall Reporting Advanced
	Multi-firewall aggregate reporting
	Save custom report templates
	Scheduled reporting
	Export reports in PDF, CFV or HTML format
	Up to 1 year data storage per firewall
	XDR/MTR connector
	Syslog search and view
	Syslog data storage in Sophos Central
	On-demand reporting in Sophos Central
	Report across multiple firewalls
	Save, export, and schedule your reports
	On-Box Reporting
	No extra charge
	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)
	Built-in storage on XGS Series for unlimited log data storage for historical reporting
	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
	Syslog Support
	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 and Support	
	Hardware warranty & RMA with Advanced Exchange
	24x7 Enhanced Plus International Support via Telephone & Email with Remote Consultation from STSE (up to 4 hrs)

	FREE Security Updates & Patches
	FREE Software Features Updates & Upgrades
Security Subscriptions - Xstream Protection Bundle	
	Xstream Protection Bundle Includes :
Xstream Protection	Base License: Networking, Wireless, Xstream Architecture, Unlimited Remote Access VPN, Site-to-Site VPN, reporting
	Network Protection: Xstream TLS and DPI engine, IPS, ATP, Security Heartbeat, SD-RED VPN, reporting
	Web Protection: Xstream TLS and DPI engine, Web Security and Control, Application Control, reporting
	Zero-Day Protection: Machine Learning and Sandboxing File Analysis, reporting
	Central Orchestration: SD-WAN VPN Orchestration, Central Firewall Advanced Reporting (30-days), MTR/XDR ready
	Enhanced Support: 24/7 support, feature updates, advanced replacement hardware warranty for term
Additional Protection Modules	
Anti-Spam & WAF	Email Protection: On-box antispam, AV, DLP, encryption
	Web Server Protection: Web Application Firewall
Additional Support Options	
Enhanced Plus Support	Enhanced Plus Support Upgrade: Upgrade your support with VIP support, HW warranty for add-ons, TAM option (extra cost)
	Sophos Central Management : Group firewall management, backup management, firmware update scheduling
	Sophos Central Firewall Reporting: Prepackaged and custom report tools with seven days cloud storage for no extra charge

Additional Protection Services, Products and Modules	
Add-On Services	Managed Threat Response: 24/7 threat hunting, detection and response delivered by an expert team
	Sophos Intercept X Endpoint with XDR: Sophos Central managed next-gen endpoint protection with EDR
	ZTNA: Sophos Central managed Zero Trust Network Access
	Central Email Advanced: Sophos Central managed antispam, AV, DLP, encryption

	License ID
	Manufacturer’s authorization form
	Warranty agreement form
	Sophos Silver Partner or Higher
	One year license (02 September 2022 - 02 September 2023)