



West Visayas State University

(Formerly Iloilo Normal School)
HIMAMAYLAN CITY CAMPUS

Brgy. Caradlo-an, Himamaylan City, Negros Occidental, 6108
* Tel.No. (034)-388-3300

* Official Page: <https://www.facebook.com/westhimamaylan/>
* Email Address: himamaylan@wvsu.edu.ph



PROCUREMENT OF FIREWALL FOR MIS TECHNICAL SPECIFICATION

Minimum Hardware:

| | |
|--------------|---|
| Form Factor | : 1U rackmount |
| Processor | : x86 AMD CPU |
| Memory | : 8 GB (2400) DDR4 |
| Hard Drive | : 1x min. 120 GB SATA-III |
| Ports | : 8x GE Copper w/ 1pair fixed bypass ports), 2x SFP GE Fiber |
| I/O Ports | : 1x COM RJ45, 2x USB 3.0 / 1x USB 2.0 / 1x RJ45 MGMT / , 1x Micro USB (cable included) / w/ 1x expansion bay |
| Display | : Multi-function LCD display |
| Power Supply | : Internal auto-ranging DC100-240VAC, 3-6A@50-60 Hz External Redundant PSU Option |

Product Certifications (Safety, EMC) : CB, CE, UL, FCC, ISED, VCCI, CCC*, KC, BSMI*, RCM, NOM, Anatel*

Max. Power-over-Ethernet (using Flexi Port module)

| | |
|------------------------|---------------------|
| 1 module | : 4 ports, 60w max. |
| Firewall Throughput | : 30,000 Mbps |
| IPS throughput | : 5,800 Mbps |
| Concurrent connections | : 6,500,000 |
| New connections/sec | : 134,700 |
| Maximum licensed users | : unrestricted |

Base Firewall Features:

- General Management
- Central Firewall Management
- Firewall, Networking & Routing
- SD-WAN
- Base Traffic Shaping & Quotas
- Secure Wireless
- ZTNA
- Authentication
- User Self-Serve Portal
- Base VPN Options
- Sophos Connect VPN Client

Network Protection

- 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
- 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
- Central management of all SD-WAN 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 SD-WAN device after a select period of inactivity
- Compression of tunnel traffic
- Integrated wireless options
- **Ultra affordable**
 - Unique encrypted HTML5 self-service portal with support for RDP, HTTP, HTTPS, SSH, Telnet, and VNC

Web Protection

- 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 OEM Labs
- 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
- 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 enforcement
- 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
- 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
- Synchronized App Control to automatically, identify, classify, and control all unknown Windows and Mac applications on the network by sharing information between
- 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
- 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

- 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
- 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 OEM Labs' 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 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.
- 30-days of cloud data storage for historical firewall reporting with advanced features to
- 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

- 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
- 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
- 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
- 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 OEM Labs

Web Server Protection Features

- 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

- 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
- Multi-firewall aggregate reporting
- Save custom report templates
- Scheduled reporting
- Export reports in PDF, CSV 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
- 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 - Protection Bundle:

| | |
|-----------------------|--|
| Base License | : Networking, Wireless, Architecture, Unlimited Remote Access VPN, Site-to-Site VPN, reporting |
| Network Protection | : TLS and DPI engine, IPS, ATP, Security Heartbeat, SD-RED VPN, reporting |
| Web Protection | : 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 |

Sophos Central Management and Reporting (included at no charge)

| | |
|------------------------------------|---|
| 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 |

Others:

1. Standard 8x5 Technical support through Phone, Email and Remote Web Assistance
2. Hardware warranty and replacement in case of failure
3. Delivery, Implementation, Documentation and Training
4. Minimum of 2-years Protection Subscription
5. 2 years Warranty

Estimated Cost: PHP 500,000.00

Conditions:

1. Bidder should submit a certificate of authorization from the manufacturer that they are authorized partner or reseller to extend the maximum warranty of all equipment.
2. The bidder should have a Certified Engineer of the brand they are offering. Shall submit a non-expired certification
3. Contractor shall provide a minimum of 8hours In-House Training/Knowledge transfer for the Network Administrator.

Documentation:

1. The manufacturer should provide certificate of ownership of license that license should be WVSU-Himamaylan City Campus
2. Contractor shall ensure that the configuration and implementation should be as per the requirement of the end-user.
3. Proper Documentation and over-all design transfer is part of the submittals before final acceptance of the project.

Prepared By:



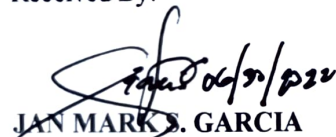
KURT HARVEY B. DEASIS
Network Administrator
MIS in Charge

Conformed By:



MARLYN V. RIVERA, Ph.D.
End-User

Received By:



JAN MARK S. GARCIA
TWG - IT Equipment