West Visayas State University

(Formerly Iloilo Normal School)
Procurement Division/ Bids and Awards Committee Secretariat Office
Luna St., La Paz, Iloilo City 5000
Iloilo, Philippines
* Trunkline: (063) (033) 320-0870 loc1103/1104 * Telefax No.: (033) 320-0879
* Website: www.wvsu.edu.ph * Email Address: bac@wvsu.edu.ph

SUPPLEMENTAL/BID BULLETIN

Project Reference No.	***IB No. 2023-38***
Name of the Project	***Procurement of Next - Generation Firewall***
Location of the Project	***WVSU - Main Campus***

ADDENDUM NO. 2023-30
September 13, 2023

This **Addendum No. 2023-30** is issued to modify the **Section VII. Technical Specifications.** This shall form an integral part of the Bidding Documents.

I. Section VII. Technical Specifications:

Item No.	Description	Corrections/ Amendments/ Instructions
1.	***NEXT-GENERATION FIREWALL***	***NEXT-GENERATION FIREWALL***
	Qty/ Unit: 1 lot	***Qty/ Unit: 1 lot***
	Pls. specify brand and model:	***Pls. specify brand and model:***
	Unit Cost: 5,000,000.00	***Unit Cost: 5,000,000.00***
	Next-generation firewalls (NGFWs) are advanced network security solutions designed to provide more sophisticated and comprehensive protection compared to traditional firewalls. They incorporate various features and capabilities to address the evolving threat landscape and the complexities of modern network environments. Some key features of next-generation firewalls include:	*Next-generation firewalls (NGFWs) are advanced network security solutions designed to provide more sophisticated and comprehensive protection compared to traditional firewalls. They incorporate various features and capabilities to address the evolving threat landscape and the complexities of modern network environments. Some key features of next-generation firewalls include:*
	• *Application Awareness and Control*	• *Application Awareness and Control*
	• *Intrusion Prevention System (IPS*	• *Intrusion Prevention System (IPS*
	• *User Identity and Access Control*	• *User Identity and Access Control*
	• *Content Filtering*	• *Content Filtering*
	• *Advanced Threat Protection*	• *Advanced Threat Protection*
	• *SSL/TLS Inspection*	• *SSL/TLS Inspection*
	• *Geolocation Filtering*	• *Geolocation Filtering*
	• *Quality of Service (QoS) and Bandwidth Management*	• *Quality of Service (QoS) and Bandwidth Management*
	• *Integration with Security Information and Event Management (SIEM) Systems*	• *Integration with Security Information and Event Management (SIEM) Systems*
	• *Threat Intelligence Integration*	• *Threat Intelligence Integration*
	• *Network Segmentation*	• *Network Segmentation*
	• *Remote Access VPN*	• *Remote Access VPN*
	Item 1. Next Generation Firewall	***Item 1. Next Generation Firewall***
	• *Dimension : 1U or 2U*	• *Dimension : 1U or 2U*
	• *Memory : At least 48G*	• *Memory : At least 48G*
	• *Storage : At least 128GB SSD + 960G SSD*	• *Storage : At least 128GB SSD + 960G SSD*
	• *Ports : At least 4*GE RJ45 + 4*1G Fiber SFP + 8*10GFiber SFP+ and 4* NIC slot*	• *Ports : At least 4*GE RJ45 + 4*1G Fiber SFP + 8*10GFiber SFP+ and 4* NIC slot*
	• *I/O Ports : At least 2*USB + 1*RJ45 MGMT*	• *I/O Ports : At least 2*USB + 1*RJ45 MGMT*
	• *Power Supply : Dual Power Supplies*	• *Power Supply : Dual Power Supplies*
	• *Certifications (Safety, EMC) : CE, FCC, ROHS*	• *Certifications (Safety, EMC) : CE, FCC, ROHS*
	• *Firewall Throughput : 80,000 Mbps*	• *Firewall Throughput : 80,000 Mbps*
	• *NGFW Throughput : 32,000 Mbps*	• *NGFW Throughput : 32,000 Mbps*
	• *Threat Protection Throughput : 18,000 Mbps*	• *Threat Protection Throughput : 18,000 Mbps*
	• *Concurrent connections : 27,000,000*	• *Concurrent connections : 27,000,000*
	• *IPsec VPN Throughput : 12,500 Mbps*	• *IPsec VPN Throughput : 12,500 Mbps*
	• *New connections : 700,000*	• *New connections : 700,000*
	• *License: Premium Subscribed Features*	• *License: Premium Subscribed Features minimum*

	minimum of 5 Years	*of 5 Years*
	Features	***Features***
	Network Adaptability	***Network Adaptability***
	• *Should support the following deployment modes: Routing/gateway/Layer3 mode; Transparent/Layer2/Inline mode; Virtual wire mode; Bypass mode; Mixed mode.*	• *Should support the following deployment modes: Routing/gateway/Layer3 mode; Transparent/Layer2/Inline mode; Virtual wire mode; Bypass mode; Mixed mode.*
	• *Must support high availability via: Active-Active mode; Active-Passive or Active Standby mode.*	• *Must support high availability via: Active-Active mode; Active-Passive or Active Standby mode.*
	• *Should support: Vlan Interface (802.1Q); Sub-Interface.*	• *Should support: Vlan Interface (802.1Q); Sub-Interface.*
	• *Must support different mode of NAT: SNAT, DNAT and bidirection NAT; One to one NAT, one to many, many to one, many to many NAT; NAT46, NAT64.*	• *Must support different mode of NAT: SNAT, DNAT and bidirection NAT; One to one NAT, one to many, many to one, many to many NAT; NAT46, NAT64.*
	• *Should support DHCP, include Support DHCP server, DHCP relay; Support IP reservation.*	• *Should support DHCP, include Support DHCP server, DHCP relay; Support IP reservation.*
	Routing	***Routing***
	• *Must support static routing.*	• *Must support static routing.*
	• *Must support dynamic routing protocol: IPv4 Network (RIPv1/2, OSPFv2, BGP4); IPv6 Network (OSPFv3).*	• *Must support dynamic routing protocol: IPv4 Network (RIPv1/2, OSPFv2, BGP4); IPv6 Network (OSPFv3).*
	• *Support redistribute direct route, static route, RIP route (OSPFv2 only) and default route to OSPF.*	• *Support redistribute direct route, static route, RIP route (OSPFv2 only) and default route to OSPF.*
	• *Must support policy-based route. The policy route can setup with: Routing source can be specific to IP, IP group; Support select route based on IP, services, Country/Region, Application etc.; Support load balance via at least 4 methods: Round Robin, Bandwidth ratio Round robin, Weighted least traffic, prefer the first link (link on top).*	• *Must support policy-based route. The policy route can setup with: Routing source can be specific to IP, IP group; Support select route based on IP, services, Country/Region, Application etc.; Support load balance via at least 4 methods: Round Robin, Bandwidth ratio Round robin, Weighted least traffic, prefer the first link (link on top).*
	IPsec VPN	***IPsec VPN***
	• *Must be able to setup site to site VPN in the following scenarios: Both site is static IP; Both site is dynamic IP; One site is dynamic IP while the other site is static IP.*	• *Must be able to setup site to site VPN in the following scenarios: Both site is static IP; Both site is dynamic IP; One site is dynamic IP while the other site is static IP.*
	• *Must support IKEv1 and IKEv2.*	• *Must support IKEv1 and IKEv2.*
	• *Must support the following algorithm with IPsec VPN: Support ESP, AH; Encryption Algorithm: DES, 3DES, AES (128), AES192, AES256, SANGFOR_DES; Hash Algorithm: MD5, SHA1, SHA2-256, SHA2-384, SHA2-512; Support Perfect Forward Secrecy, group1, group2, group5, group14, group15, group16, group17, group18.*	• *Must support the following algorithm with IPsec VPN: Support ESP, AH; Encryption Algorithm: DES, 3DES, AES (128), AES192, AES256, SANGFOR_DES; Hash Algorithm: MD5, SHA1, SHA2-256, SHA2-384, SHA2-512; Support Perfect Forward Secrecy, group1, group2, group5, group14, group15, group16, group17, group18.*
	• *Should support SD-WAN capability via VPN tunnels: Support session based link balancing mode; Can choose the optimize link based on bandwidth-remaining ratio, application type or link quality (means packet loss, jitter, latency).*	• *Should support SD-WAN capability via VPN tunnels: Support session based link balancing mode; Can choose the optimize link based on bandwidth-remaining ratio, application type or link quality (means packet loss, jitter, latency).*
	• *Support monitoring the status of each VPN tunnel, the data be monitoring includes: Overview of all the active VPN tunnels; Inbound/outbound traffic; Latency; Packet loss rate.*	• *Support monitoring the status of each VPN tunnel, the data be monitoring includes: Overview of all the active VPN tunnels; Inbound/outbound traffic; Latency; Packet loss rate.*
	SSL VPN	***SSL VPN***
	• *Should support SSL VPN features: Support at least 30 concurrent user access; Support TCP, UDP, ICMP protocols; Support HTTP, HTTPS, Email, Fileshare, FTP etc.; Support control access by IP, URL, TCP/UDP port etc.; Support access resource (destination IP/system) by NAT (NGAF IP address)*	• *Should support SSL VPN features: Support at least 30 concurrent user access; Support TCP, UDP, ICMP protocols; Support HTTP, HTTPS, Email, Fileshare, FTP etc.; Support control access by IP, URL, TCP/UDP port etc.; Support access resource (destination IP/system) by NAT (NGAF IP address)*

	or virtual IP.	*or virtual IP.*
	• *Should be able to support SSL VPN on system below: Windows XP/7/8/10/11; MacOS 10.9 - MacOS 11.x & Apple M1; Andriod 4.x - Andriod 9.0; IOS7.x - IOS12.x.*	• *Should be able to support SSL VPN on system below: Windows XP/7/8/10/11; MacOS 10.9 - MacOS 11.x & Apple M1; Andriod 4.x - Andriod 9.0; IOS7.x - IOS12.x.*
	• *Should be able to support SSL VPN with mainstream browsers, include IE、Firefox、Chrome, Edge, Safari, Opera etc.*	• *Should be able to support SSL VPN with mainstream browsers, include IE、Firefox、Chrome, Edge, Safari, Opera etc.*
	• *Should be able to support: local user database; LDAP, Radius authentication; Two-Factor authentication by SMS, TOTP (Google/Microsoft authenticator); Hardware ID.*	• *Should be able to support: local user database; LDAP, Radius authentication; Two-Factor authentication by SMS, TOTP (Google/Microsoft authenticator); Hardware ID.*
	• *Must support following algorithms: Hash (MD5, SHA-1, SHA2-256, SHA2-384, SHA2-512); Encryption (AES, AES192, AES256, DES, 3DES; Authentication (RSA).*	• *Must support following algorithms: Hash (MD5, SHA-1, SHA2-256, SHA2-384, SHA2-512); Encryption (AES, AES192, AES256, DES, 3DES; Authentication (RSA).*
	Access Control	***Access Control***
	• *Should support the application control feature and meet the following specifications: Support application control and can identify & control over 9000 applications; Support admin customize their own application types; Typical types of applications that can be controlled include games, P2P, shopping, social networking, etc.; Should be able to control applications via source/destination IP, username, schedule, etc.; Be able to deny, allow user behavior by applications.*	• *Should support the application control feature and meet the following specifications: Support application control and can identify & control over 9000 applications; Support admin customize their own application types; Typical types of applications that can be controlled include games, P2P, shopping, social networking, etc.; Should be able to control applications via source/destination IP, username, schedule, etc.; Be able to deny, allow user behavior by applications.*
	• *Must support URL filtering: Provide at least 70+ URL categories, include game, gambling, finance, Pornography etc.; Support manually create customized the URL category; Should provide on-premise URL signature database, not only rely on cloud.*	• *Must support URL filtering: Provide at least 70+ URL categories, include game, gambling, finance, Pornography etc.; Support manually create customized the URL category; Should provide on-premise URL signature database, not only rely on cloud.*
	• *Must support filter, which can filter the download, upload file by file type(extension); Support common file type(extension) category, including, image, text, executable file, scripts etc.; Support customized file type(extension).*	• *Must support filter, which can filter the download, upload file by file type(extension); Support common file type(extension) category, including, image, text, executable file, scripts etc.; Support customized file type(extension).*
	• *Should support feature to control concurrent sessions/connections: Be able to control concurrent session/connect by source IP, destination IP, or bidirectional; In the policy, it will be able to set the maximum concurrent session/connection number per IP.*	• *Should support feature to control concurrent sessions/connections: Be able to control concurrent session/connect by source IP, destination IP, or bidirectional; In the policy, it will be able to set the maximum concurrent session/connection number per IP.*
	• *Should be able to control traffic based on Geolocations: Be able to control the source IP by a geolocation level, that means the device have a database that can identify the access (IP) is from which country/region and specify the deny or allow action.*	• *Should be able to control traffic based on Geolocations: Be able to control the source IP by a geolocation level, that means the device have a database that can identify the access (IP) is from which country/region and specify the deny or allow action.*
	• *Must be able to support bandwidth management feature: Be able to limit or guarantee the bandwidth based on IP, user, application, schedule, vlan, country etc.; Be able to control maximum bandwidth of per IP/User; Support bandwidth control for both upload and download; Support bandwidth usage status monitoring; Traffic ranking based on username, applications or IP.*	• *Must be able to support bandwidth management feature: Be able to limit or guarantee the bandwidth based on IP, user, application, schedule, vlan, country etc.; Be able to control maximum bandwidth of per IP/User; Support bandwidth control for both upload and download; Support bandwidth usage status monitoring; Traffic ranking based on username, applications or IP.*
	Intrusion Prevention System	***Intrusion Prevention System***
	• *Must support vulnerability database with at least 9000+ entries.*	• *Must support vulnerability database with at least 9000+ entries.*
	• *Must support separate server and endpoint*	• *Must support separate server and endpoint*

	vulnerability database group for convenient policy configuration. • *Must be able to block worms, Trojans, spyware, scanning, DoS, DDoS, vulnerability exploits, buffer overflow attacks, abnormal protocol and attacks with evasive tactic employed.*	*vulnerability database group for convenient policy configuration.* • *Must be able to block worms, Trojans, spyware, scanning, DoS, DDoS, vulnerability exploits, buffer overflow attacks, abnormal protocol and attacks with evasive tactic employed.*
	• *Support burp-force attack prevention for FTP, IMAP MSSQL, POP3 SMTP, ORACLE, RDP, SMBv1, SMBv2, SMBv3, etc.*	• *Support burp-force attack prevention for FTP, IMAP MSSQL, POP3 SMTP, ORACLE, RDP, SMBv1, SMBv2, SMBv3, etc.*
	APT Prevention	***APT Prevention***
	• *Must support APT detection of identifying botnet, remote control trojans, malicious link, and other threats.*	• *Must support APT detection of identifying botnet, remote control trojans, malicious link, and other threats.*
	• *Must support anti-malware database with more than 400,000+ entries.*	• *Must support anti-malware database with more than 400,000+ entries.*
	• *Must be able to conduct cross-module intelligent correction of IPS and APT detection module, that to generate temporary FW rules to lock the suspicious IP when malicious behavior from that IP is detected by any of the modules.*	• *Must be able to conduct cross-module intelligent correction of IPS and APT detection module, that to generate temporary FW rules to lock the suspicious IP when malicious behavior from that IP is detected by any of the modules.*
	• *Support effectively distinguish the hazardous traffic flow in the common application of the RDP, SSL, IMAP, SMTP, POP3, FTP, DNS, HTTP, WEB, and so on traffic flow , but also can be used for the normal operation of non-standard port for early warning.*	• *Support effectively distinguish the hazardous traffic flow in the common application of the RDP, SSL, IMAP, SMTP, POP3, FTP, DNS, HTTP, WEB, and so on traffic flow , but also can be used for the normal operation of non-standard port for early warning.*
	• *Support in-depth analysis on detected malware or trojan behaviors by demonstrating interaction & communication between external C&C botnets and others suspicious events.*	• *Support in-depth analysis on detected malware or trojan behaviors by demonstrating interaction & communication between external C&C botnets and others suspicious events.*
	Risk Assessment and Prevention	***Risk Assessment and Prevention***
	• *Must provide risk assessment module that allows to scan and identify security loopholes such as open port, system vulnerabilities, weak passwords and other risks of the protected servers.*	• *Must provide risk assessment module that allows to scan and identify security loopholes such as open port, system vulnerabilities, weak passwords and other risks of the protected servers.*
	• *Must support real-time vulnerability analysis, includes the underlying software vulnerability analysis, generate real-time analysis report. That can be deployed in mirror mode to discover system vulnerabilities within protected network in real-time.*	• *Must support real-time vulnerability analysis, includes the underlying software vulnerability analysis, generate real-time analysis report. That can be deployed in mirror mode to discover system vulnerabilities within protected network in real-time.*
	• *The real-time vulnerability is also to support to detect for the website if it existed backlink, and we can record the type of the black link and the location of backlink.*	• *The real-time vulnerability is also to support to detect for the website if it existed backlink, and we can record the type of the black link and the location of backlink.*
	• *Risk assessment and scanning results must be shown and generated with corresponding reports with detailed description of the issues and recommended solution.*	• *Risk assessment and scanning results must be shown and generated with corresponding reports with detailed description of the issues and recommended solution.*
	• *Must be able to actively push the current popular 0 day or high-risk vulnerabilities, and can provide vulnerability detection tools for business scan, according to the results of scan, it can generate safety protection policies.*	• *Must be able to actively push the current popular 0 day or high-risk vulnerabilities, and can provide vulnerability detection tools for business scan, according to the results of scan, it can generate safety protection policies.*
	Data Breach Prevention	***Data Breach Prevention***
	• *Allow to define multiple types of sensitive information based on the characteristics of stored data, the sensitive information includes email account information, MD5 encrypted passwords.*	• *Allow to define multiple types of sensitive information based on the characteristics of stored data, the sensitive information includes email account information, MD5 encrypted passwords.*
	• *Must be able to restrict suspicious file downloading with file types of dat, bak,dmp,backup, asa,log, fp, frx, frt, CNF, ade,mde, db, ldb,etc.*	• *Must be able to restrict suspicious file downloading with file types of dat, bak,dmp,backup, asa,log, fp, frx, frt, CNF, ade,mde, db, ldb,etc.*

	Anti-Virus	***Anti-Virus***
	• *Stream-based anti-virus for HTTP, FTP, SMTP and POP3 , SMBv3 protocols, etc.*	• *Stream-based anti-virus for HTTP, FTP, SMTP and POP3 , SMBv3 protocols, etc.*
	• *Must support built-in Artificial Intelligence capability to detect malware, virus and ransomware virants and provide the malware analysis report.*	• *Must support built-in Artificial Intelligence capability to detect malware, virus and ransomware virants and provide the malware analysis report.*
	• *Should support compressed file malware inspection, up to 16 layers.*	• *Should support compressed file malware inspection, up to 16 layers.*
	Reporting	***Reporting***
	• *Must support built-in report center, which provides comprehensive security analyzing reports including but not limit to attack trends by "All attacks" and "Valid Attacks"; Security rating by "business server security", "user security" and "vulnerability" ; Business server security by suffered attack times ranking ; Vulnerability assessment.*	• *Must support built-in report center, which provides comprehensive security analyzing reports including but not limit to attack trends by "All attacks" and "Valid Attacks"; Security rating by "business server security", "user security" and "vulnerability" ; Business server security by suffered attack times ranking ; Vulnerability assessment.*
	• *Support the detailed loges for security issues as DOS attack, IPS, viruses, website access, application control, user login and OS configuration.*	• *Support the detailed loges for security issues as DOS attack, IPS, viruses, website access, application control, user login and OS configuration.*
	• *Support detailed threats analysis for specific attack by Description, Target, Solution, Support security analysis for specific server with Attack type, Attack source, etc.*	• *Support detailed threats analysis for specific attack by Description, Target, Solution, Support security analysis for specific server with Attack type, Attack source, etc.*
	• *The report center must provide full visibility to network, endpoint clients and the business servers with multi-dimensional analysis of risks, vulnerabilities, attacks, threats, traffic and behaviors.*	• *The report center must provide full visibility to network, endpoint clients and the business servers with multi-dimensional analysis of risks, vulnerabilities, attacks, threats, traffic and behaviors.*
	• *Support PDF format and automatically send to pre-defined mailbox on daily/weekly/monthly basis.*	• *Support PDF format and automatically send to pre-defined mailbox on daily/weekly/monthly basis.*
	Real-time Monitoring	***Real-time Monitoring***
	• *Real time provides CPU, memory, disk usage, session number, the number of online users, the network interface, box resource information.*	• *Real time provides CPU, memory, disk usage, session number, the number of online users, the network interface, box resource information.*
	• *Must be provide real-time user ranking / real-time application ranking / real-time host ranking.*	• *Must be provide real-time user ranking / real-time application ranking / real-time host ranking.*
	• *Must be provide real-time attack map, include top attack country and counting, real-time attack and threat detail.*	• *Must be provide real-time attack map, include top attack country and counting, real-time attack and threat detail.*
	• *Provide information security incidents, including recently security incidents, server security incidents, terminal security incidents.*	• *Provide information security incidents, including recently security incidents, server security incidents, terminal security incidents.*
	• *In security status, it displays the current network risks need to be handled, and top attacks, bots show the threat stage and security rating.*	• *In security status, it displays the current network risks need to be handled, and top attacks, bots show the threat stage and security rating.*
	• *Top session can display Real-time, Last 24 hours, Last 7 days of the current session and the new session.*	• *Top session can display Real-time, Last 24 hours, Last 7 days of the current session and the new session.*
	Certifications	***Certifications***
	• *Vendors must be at Visionaries or higher level of Gartner Magic Quadrant for Network Firewalls.*	• *Vendors must be at Visionaries or higher level of Gartner Magic Quadrant for Network Firewalls.*
	• *Vendors must have AAA Rating at Cyberdating's Enterprise Firewall also be reported as 2023 Recommended Enterprise Firewalls.*	• *Vendors must have AAA Rating at Cyberdating's Enterprise Firewall also be reported as 2023 Recommended Enterprise Firewalls.*
	Item 2. Identity and Access Management	***Item 2. Identity and Access Management***
	• *Dimension : 1U or 2U*	• *Dimension : 1U or 2U*
	• *Memory : At least 8G*	• *Memory : At least 8G*

	• *Storage : At least 64 GB SSD + 960 GB SSD*	• *Storage : At least 64 GB SSD + 960 GB SSD*
	• *Ports : At least 6*10/100/1000 Base-T and 2*10 Fiber SFP+ Interface, 3 pair of Bypass (copper) network interface*	• *Ports : At least 6*10/100/1000 Base-T and 2*10 Fiber SFP+ Interface, 3 pair of Bypass (copper) network interface*
	• *I/O Ports : 2*USB*	• *I/O Ports : 2*USB*
	• *Power Supply : Dual Power Supplies*	• *Power Supply : Dual Power Supplies*
	• *Layer 7 Throughput : 2Gbps*	• *Layer 7 Throughput : 2Gbps*
	• *Concurrent user : 15,000*	• *Concurrent user : 15,000*
	• *License : Essential Bundle (Bandwidth Management, User Authentication, URL Filtering, Traffic Control, User Behavior Audit, Content Audit, Proxy Server, Anti-proxy, Endpoints Management minimum of 5 Years*	• *License : Essential Bundle (Bandwidth Management, User Authentication, URL Filtering, Traffic Control, User Behavior Audit, Content Audit, Proxy Server, Anti-proxy, Endpoints Management minimum of 5 Years*
	Features:	***Features:***
	User Authentication and Management	***User Authentication and Management***
	• *Must support ability to identify user base on IP, MAC, hostname.*	• *Must support ability to identify user base on IP, MAC, hostname.*
	• *Must support import user accounts information via CSV file, and support synchronize users with LDAP, database and H3C CAMS Server.*	• *Must support import user accounts information via CSV file, and support synchronize users with LDAP, database and H3C CAMS Server.*
	• *Must support password based on SMS, Webchat, QR code, Facebook, LDAP, RADIUS, POP3, CAS, H3C CAMS, OAUTH, SAML 2.0 authentication.*	• *Must support password based on SMS, Webchat, QR code, Facebook, LDAP, RADIUS, POP3, CAS, H3C CAMS, OAUTH, SAML 2.0 authentication.*
	• *Must support single sign-on authentication base on Active Directory, Radius, POP3, Proxy, Web Server, HTTP API, Database Server. Support integration with SMS authentication, Facebook authentication, WeChat authentication, QR code authentication, and other popular authentication methods.*	• *Must support single sign-on authentication base on Active Directory, Radius, POP3, Proxy, Web Server, HTTP API, Database Server. Support integration with SMS authentication, Facebook authentication, WeChat authentication, QR code authentication, and other popular authentication methods.*
	• *Support list of protocol as a third-party appliance for authentication including CMCC1.0, CMCC2.0, Portal 2.0/IMC, Cisco Web Portal Protocol and Aruba.*	• *Support list of protocol as a third-party appliance for authentication including CMCC1.0, CMCC2.0, Portal 2.0/IMC, Cisco Web Portal Protocol and Aruba.*
	• *User can submit the application information, and then IT administrator can approve the application, support add new item of information collection.*	• *User can submit the application information, and then IT administrator can approve the application, support add new item of information collection.*
	Access Control	***Access Control***
	• *Application Database must support more than 6000+ applications in its database including 700+ cloud applications, 1000+ mobile applications, 300+ web applications and must support self-define app rules, application database update in every 2 weeks.*	• *Application Database must support more than 6000+ applications in its database including 700+ cloud applications, 1000+ mobile applications, 300+ web applications and must support self-define app rules, application database update in every 2 weeks.*
	• *Must support access management based on services or ports such as HTTP (80), HTTPS (443), TELNET(23), SSH(22), FTP(21), SMTP(25), POP3(110).*	• *Must support access management based on services or ports such as HTTP (80), HTTPS (443), TELNET(23), SSH(22), FTP(21), SMTP(25), POP3(110).*
	• *Must support ten million URLs of URL database, must include sub categories such as pornographic, gambling, games, illegal drugs, counteraction, financial, education in URL database.*	• *Must support ten million URLs of URL database, must include sub categories such as pornographic, gambling, games, illegal drugs, counteraction, financial, education in URL database.*
	• *Must support control HTTP, FTP upload and download activity based on file type at least docx, xlsx, pptx, txt, rar, bat, exe, pdf, zip, rar, gz, bz2, Z, tgz, tbz, 7z, cab, bz.*	• *Must support control HTTP, FTP upload and download activity based on file type at least docx, xlsx, pptx, txt, rar, bat, exe, pdf, zip, rar, gz, bz2, Z, tgz, tbz, 7z, cab, bz.*

	Bandwidth Management	***Bandwidth Management***
	• *Must support guarantee and limit bandwidth management, support at least 1000 policy.*	• *Must support guarantee and limit bandwidth management, support at least 1000 policy.*
	• *Must support BM base on application types, website types, file types, users, schedules, destination IP, end point types (PC, mobile phone).*	• *Must support BM base on application types, website types, file types, users, schedules, destination IP, end point types (PC, mobile phone).*
	• *Support Dynamic bandwidth management, support average allocation/predefined bandwidth allocation among users in a single traffic pipe.*	• *Support Dynamic bandwidth management, support average allocation/predefined bandwidth allocation among users in a single traffic pipe.*
	• *Support precise identification and manage known, variant, encrypted and unknown P2P behaviors. Support application at least Xunlei P2P, BT, eMule, Ares, BitTorrent sync, P2P-NAT, P2P Behavior.*	• *Support precise identification and manage known, variant, encrypted and unknown P2P behaviors. Support application at least Xunlei P2P, BT, eMule, Ares, BitTorrent sync, P2P-NAT, P2P Behavior.*
	• *Support with precise identify and manage international bandwidth. Make overseas traffic visible. Manage regional and overseas traffic respectively. Control overseas traffic.*	• *Support with precise identify and manage international bandwidth. Make overseas traffic visible. Manage regional and overseas traffic respectively. Control overseas traffic.*
	Report Center	***Report Center***
	• *Support logs search base on time, IP address, endpoint device, application flow, action.*	• *Support logs search base on time, IP address, endpoint device, application flow, action.*
	• *Support application traffic ranking, URL category traffic ranking, URL traffic ranking, application duration ranking, URL category traffic ranking, URL traffic ranking, file upload ranking, IM ranking, Email and microblog ranking, term search ranking, endpoint device ranking*	• *Support application traffic ranking, URL category traffic ranking, URL traffic ranking, application duration ranking, URL category traffic ranking, URL traffic ranking, file upload ranking, IM ranking, Email and microblog ranking, term search ranking, endpoint device ranking*
	• *Support application access trend, URL category access trend, TOP talks of URL trend, endpoint access trend.*	• *Support application access trend, URL category access trend, TOP talks of URL trend, endpoint access trend.*
	• *Support Real-time monitor of CPU / hard disk / traffic / connection / session status, online user information, traffic ranking, connection ranking; real-time utilization visibility of bandwidth channels.*	• *Support Real-time monitor of CPU / hard disk / traffic / connection / session status, online user information, traffic ranking, connection ranking; real-time utilization visibility of bandwidth channels.*
	• *Support Content log including IM chat (Gtalk, Skype, QQ, Yahoo! Messenger); SMTP and Web mail content and attachment (Gmail, Yahoo, exchange), keyword search (Google, Bing).*	• *Support Content log including IM chat (Gtalk, Skype, QQ, Yahoo! Messenger); SMTP and Web mail content and attachment (Gmail, Yahoo, exchange), keyword search (Google, Bing).*
	• *Support customize report base on traffic, online duration, Internet activities, URL category, endpoint.*	• *Support customize report base on traffic, online duration, Internet activities, URL category, endpoint.*
	• *Support report file format CSV, PDF and able to integrate with external storage with specific data format for advanced use;*	• *Support report file format CSV, PDF and able to integrate with external storage with specific data format for advanced use;*
	Business Intelligence	***Business Intelligence***
	• *Analyze and visualize Internet bandwidth usage including bandwidth overload analysis, bandwidth-intensive application distribution and tracking of the most active applications and users, offering intuitive insight on bandwidth utilization.*	• *Analyze and visualize Internet bandwidth usage including bandwidth overload analysis, bandwidth-intensive application distribution and tracking of the most active applications and users, offering intuitive insight on bandwidth utilization.*
	• *Use to visualize load and throughput on leased lines, as well as real time traffic ranking by application and user, providing more comprehensive information for administrators responsible on expansion of leased line bandwidth.*	• *Use to visualize load and throughput on leased lines, as well as real time traffic ranking by application and user, providing more comprehensive information for administrators responsible on expansion of leased line bandwidth.*
	• *Identify and analyze office PC electricity waste and estimate costs by user or department, making the IT department more productive and valuable in cooperative operations.*	• *Identify and analyze office PC electricity waste and estimate costs by user or department, making the IT department more productive and valuable in cooperative operations.*

	Management Tools	***Management Tools***
	• *Must support redirect user URL request to specific page, with configuration of authentication.*	• *Must support redirect user URL request to specific page, with configuration of authentication.*
	• *Must support flow quota base on daily and monthly, support concurrent session quota per user.*	• *Must support flow quota base on daily and monthly, support concurrent session quota per user.*
	• *Must support hierarchical administrator privileges. Functionality of different modules can be assigned to different administrators as needed, via a hierarchical management model; Administration of different functions and modules can be delegated to different administrative groups.*	• *Must support hierarchical administrator privileges. Functionality of different modules can be assigned to different administrators as needed, via a hierarchical management model; Administration of different functions and modules can be delegated to different administrative groups.*
	• *Must support management base on endpoint device OS, identify the type of endpoints and manage the endpoints, support detected endpoint for access control policy based on endpoint type i.e mobile device, pc, dumb endpoint, medical equipment and custom device.*	• *Must support management base on endpoint device OS, identify the type of endpoints and manage the endpoints, support detected endpoint for access control policy based on endpoint type i.e mobile device, pc, dumb endpoint, medical equipment and custom device.*
	Network and Deployment	***Network and Deployment***
	• *Must support built-in stateful Firewall; Built-in IPsec VPN; Gateway Anti-virus option.*	• *Must support built-in stateful Firewall; Built-in IPsec VPN; Gateway Anti-virus option.*
	• *Support flexible deployment mode at least Route, Bridge, Double bridge, Bypass, Single-arm mode.*	• *Support flexible deployment mode at least Route, Bridge, Double bridge, Bypass, Single-arm mode.*
	• *Support high availability active-standy and active-active mode.*	• *Support high availability active-standy and active-active mode.*
	• *Must support IPv6, include authentication, application, bandwidth management, content audit and report.*	• *Must support IPv6, include authentication, application, bandwidth management, content audit and report.*
	Proxy Avoidance Protection	***Proxy Avoidance Protection***
	• *Support multiple management of proxy avoidance protection, identify the users who are using proxy avoidance applications surfing the Internet as well as block and alert users who are using proxy avoidance applications.*	• *Support multiple management of proxy avoidance protection, identify the users who are using proxy avoidance applications surfing the Internet as well as block and alert users who are using proxy avoidance applications.*
	• *Must support detection and blocking proxy avoidance applications capability via gateway and endpoint client perspective. These methods can be applied either one or both concurrently.*	• *Must support detection and blocking proxy avoidance applications capability via gateway and endpoint client perspective. These methods can be applied either one or both concurrently.*
	• *User can configure separate whitelisting of DNS server addresses, IP addresses and domains.*	• *User can configure separate whitelisting of DNS server addresses, IP addresses and domains.*
	• *Support wide range of proxy avoidance applications such as Betternet, ExpressVPN, Freegate, Hide Me, Hotspot Shield, OpenVPN, ProtonVPN, Psiphon, PureVPN, Surfshark, Tor Browser, TunnelBear, Ultrasurf and etc.*	• *Support wide range of proxy avoidance applications such as Betternet, ExpressVPN, Freegate, Hide Me, Hotspot Shield, OpenVPN, ProtonVPN, Psiphon, PureVPN, Surfshark, Tor Browser, TunnelBear, Ultrasurf and etc.*
	• *Support list of proxy avoidance applications logging and reporting purpose such as username, type of endpoint devices, proxy avoidance applications, time and etc.*	• *Support list of proxy avoidance applications logging and reporting purpose such as username, type of endpoint devices, proxy avoidance applications, time and etc.*
	• *Support integration option including on-premise and cloud endpoint client management.*	• *Support integration option including on-premise and cloud endpoint client management.*
	Asset Management	***Asset Management***
	• *Support asset inventory, check connected, offline and vacant endpoint based on ip address pool, allow to define offline status based on customise of inactive days.*	• *Support asset inventory, check connected, offline and vacant endpoint based on ip address pool, allow to define offline status based on customise of inactive days.*
	• *Support detection on unknown & rogue endpoint, support endpoint discovery and scanning based on ip address, ip address range and ip address subnet.*	• *Support detection on unknown & rogue endpoint, support endpoint discovery and scanning based on ip address, ip address range and ip address subnet.*
	• *Support endpoint device classification based on mobile device, pc, dumb endpoint, medical equipment and custom device.*	• *Support endpoint device classification based on mobile device, pc, dumb endpoint, medical equipment and custom device.*

	Ingress Client and Audit	***Ingress Client and Audit***
	• *Support content audit capabilities for various list of web (without ingress client) and local installed applications.*	• *Support content audit capabilities for various list of web (without ingress client) and local installed applications.*
	• *Support audit content and attachments, with drop-down list selection to perform "Audit" and "Do not audit" and array of file type selection support in audit capabilities.*	• *Support audit content and attachments, with drop-down list selection to perform "Audit" and "Do not audit" and array of file type selection support in audit capabilities.*
	• *Support tracing user action perform in USB devices including insert, modify file and copy file.*	• *Support tracing user action perform in USB devices including insert, modify file and copy file.*
	• *Support peripheral control, illegal external control, USB disk drive audit and IM chat audit in offline environment.*	• *Support peripheral control, illegal external control, USB disk drive audit and IM chat audit in offline environment.*
	Endpoint Compliance Security Check	***Endpoint Compliance Security Check***
	•*Support verification of local installed antivirus software within endpoint, existing antivirus version requirements and existing antivirus database update i.e number of days the virus database has not been updated.*	•*Support verification of local installed antivirus software within endpoint, existing antivirus version requirements and existing antivirus database update i.e number of days the virus database has not been updated.*
	• *Support verification for login from specify domain.*	• *Support verification for login from specify domain.*
	• *Support verification of required operating system, version and patch.*	• *Support verification of required operating system, version and patch.*
	• *Support verification of specific process name, window name, program path and status.*	• *Support verification of specific process name, window name, program path and status.*
	• *Support verification of access from IP address, port numbers and it can be applied on offline endpoints.*	• *Support verification of access from IP address, port numbers and it can be applied on offline endpoints.*
	• *Support verification of device types with blacklisting and whitelisting including storage device, network device, bluetooth device, camera and printer.*	• *Support verification of device types with blacklisting and whitelisting including storage device, network device, bluetooth device, camera and printer.*
	Item 3. Endpoint Security Software	***Item 3. Endpoint Security Software***
	Endpoint Management	***Endpoint Management***
	• *The antivirus must include but is not limited to: Protection software for Windows workstations, Linux workstations, Oracle, Active Directory.*	• *The antivirus must include but is not limited to: Protection software for Windows workstations, Linux workstations, Oracle, Active Directory.*
	• *The antivirus solution must be installed to at least 200 endpoints with a valid subscription for minimum of 1 year*	• *The antivirus solution must be installed to at least 200 endpoints with a valid subscription for minimum of 1 year*
	• *The anti-virus solution should have centralized management, monitoring update software. It should allow for slave servers, tools for distributing both the client agents and signature database updates to other clients, distribute all agents in a single action as well as monitor the health of the agent.*	• *The anti-virus solution should have centralized management, monitoring update software. It should allow for slave servers, tools for distributing both the client agents and signature database updates to other clients, distribute all agents in a single action as well as monitor the health of the agent.*
	• *The anti-virus solution should have capability to update databases of signatures for malicious programs and attacks. It should use the same mechanism to distribute signatures, updates, firewall policies and engine updates.*	• *The anti-virus solution should have capability to update databases of signatures for malicious programs and attacks. It should use the same mechanism to distribute signatures, updates, firewall policies and engine updates.*
	• *The anti-virus solution should provide a list of system resources that are continuously monitored indicating malware presence e.g., host files, registry.*	• *The anti-virus solution should provide a list of system resources that are continuously monitored indicating malware presence e.g., host files, registry.*
	• *The anti-virus solution should accommodate resident antivirus monitoring.*	• *The anti-virus solution should accommodate resident antivirus monitoring.*
	• *The anti-virus solution should have launching of tasks by schedule and/or just after loading the operating system.*	• *The anti-virus solution should have launching of tasks by schedule and/or just after loading the operating system.*
	• *The anti-virus solution should support virtualized environments.*	• *The anti-virus solution should support virtualized environments.*
	Anti-virus/Anti-malware Analysis	***Anti-virus/Anti-malware Analysis***
	• *The anti-virus solution should allow for simulation*	• *The anti-virus solution should allow for simulation*

	of unknown code before execution to determine malicious intent without user intervention.	*of unknown code before execution to determine malicious intent without user intervention.*
	• *The anti-virus solution should have a Heuristic analyzer that allows identification and blocking of previously unknown malware more efficiently including zero-day outbreaks.*	• *The anti-virus solution should have a Heuristic analyzer that allows identification and blocking of previously unknown malware more efficiently including zero-day outbreaks.*
	• *The anti-virus solution should have Artificial intelligence capabilities that allow identification and blocking of previously unknown malware more efficiently including zero-day outbreaks.*	• *The anti-virus solution should have Artificial intelligence capabilities that allow identification and blocking of previously unknown malware more efficiently including zero-day outbreaks.*
	• *The anti-virus solution should have Artificial intelligence capabilities that allows identification and blocking of previously unknown malware based on malware family classification.*	• *The anti-virus solution should have Artificial intelligence capabilities that allows identification and blocking of previously unknown malware based on malware family classification.*
	• *The anti-virus solution should have capability of scanning on the user's or administrator's request and according to a schedule. The primary administrator should be able to manage the whole solution while local domain administrators should manage their groups.*	• *The anti-virus solution should have capability of scanning on the user's or administrator's request and according to a schedule. The primary administrator should be able to manage the whole solution while local domain administrators should manage their groups.*
	• *The anti-virus solution should have capabilities of checking and disinfection of files in archives using the RAR, ARJ, ZIP, CAB, LHA, JAR, ICE formats up to 16 layers.*	• *The anti-virus solution should have capabilities of checking and disinfection of files in archives using the RAR, ARJ, ZIP, CAB, LHA, JAR, ICE formats up to 16 layers.*
	• *The anti-virus solution should have cloud-based technology that provides ability to receive verdicts in online mode about applications and executable files running on computer.*	• *The anti-virus solution should have cloud-based technology that provides ability to receive verdicts in online mode about applications and executable files running on computer.*
	• *The anti-virus solution should have capabilities of scanning of all scripts, developed in Microsoft Internet Explorer, as well as any WSH scripts (JavaScript, Visual Basic Script WSH scripts (JavaScript, Visual Basic Script etc.)), launched when the user works on the computer, including the Internet.*	• *The anti-virus solution should have capabilities of scanning of all scripts, developed in Microsoft Internet Explorer, as well as any WSH scripts (JavaScript, Visual Basic Script WSH scripts (JavaScript, Visual Basic Script etc.)), launched when the user works on the computer, including the Internet.*
	• *The anti-virus solution should have protection of HTTP-traffic scanning of all objects entering the user's computer through the HTTP/FTP protocol.*	• *The anti-virus solution should have protection of HTTP-traffic scanning of all objects entering the user's computer through the HTTP/FTP protocol.*
	Response	***Response***
	• *The anti-virus solution should have applications control that prevents applications from performing actions that may be dangerous for the system.*	• *The anti-virus solution should have applications control that prevents applications from performing actions that may be dangerous for the system.*
	• *The anti-virus solution should have protection against hacker attacks by using a firewall with an intrusion detection and prevention system (IDS/IPS) and network activity rules. It should also provide deep packet inspection of incoming network traffic.*	• *The anti-virus solution should have protection against hacker attacks by using a firewall with an intrusion detection and prevention system (IDS/IPS) and network activity rules. It should also provide deep packet inspection of incoming network traffic.*
	• *The anti-virus solution should control for isolation from any connected network.*	• *The anti-virus solution should control for isolation from any connected network.*
	• *The anti-virus solution should have special task for detecting vulnerabilities, with results available in reports. It should also allow for completely ad-hoc reports. (Not the Filtered reports).*	• *The anti-virus solution should have special task for detecting vulnerabilities, with results available in reports. It should also allow for completely ad-hoc reports. (Not the Filtered reports).*
	• *The anti-virus solution should have special task for detecting compliance with organization security compliance policies, with results available in reports. It should also allow for completely ad-hoc reports. (Not the Filtered reports).*	• *The anti-virus solution should have special task for detecting compliance with organization security compliance policies, with results available in reports. It should also allow for completely ad-hoc reports. (Not the Filtered reports).*
	• *The anti-virus solution should provide visual representation of allowed/unauthorized/suspicious communications between endpoint and other*	• *The anti-virus solution should provide visual representation of allowed/unauthorized/suspicious communications between endpoint and other*

	network and internet devices.	*network and internet devices.*
	• *The anti-virus solution should provide integrity checks of endpoints to include (but not limited to): for Windows endpoints include account, access control, security audit, history information protection, intrusion prevention and malicious code prevention. For Linux endpoints include account, access control, security audit, SSH policy detection, intrusion prevention and malicious code prevention.*	• *The anti-virus solution should provide integrity checks of endpoints to include (but not limited to): for Windows endpoints include account, access control, security audit, history information protection, intrusion prevention and malicious code prevention. For Linux endpoints include account, access control, security audit, SSH policy detection, intrusion prevention and malicious code prevention.*
	System Management	***System Management***
	•*The anti-virus solution should have Access via a Web console.*	•*The anti-virus solution should have Access via a Web console.*
	•*The anti-virus solution should have centralized management software for all protected resources must allow Installation of the antivirus protection system from a single distribution point as well as remote installations.*	•*The anti-virus solution should have centralized management software for all protected resources must allow Installation of the antivirus protection system from a single distribution point as well as remote installations.*
	•*The anti-virus solution should have centralized installation/update/deletion of antivirus protection software, setting, administration, viewing reports and statistical information on software operation. It should also be able to automatically update end point signatures and engines and pull status information when off the enterprise network, but internet connected.*	•*The anti-virus solution should have centralized installation/update/deletion of antivirus protection software, setting, administration, viewing reports and statistical information on software operation. It should also be able to automatically update end point signatures and engines and pull status information when off the enterprise network, but internet connected.*
	•*The anti-virus solution should have various methods of antivirus protection software installation: remote methods - RPC, GPO, net agents; local method – stand-alone installation package.*	•*The anti-virus solution should have various methods of antivirus protection software installation: remote methods - RPC, GPO, net agents; local method – stand-alone installation package.*
	•*The anti-virus solution should have vulnerability scanning for computers in the network, ability to provide reports on detected software vulnerabilities and rootkits. It should be able to run scheduled, on-demand and real time on access scans.*	•*The anti-virus solution should have vulnerability scanning for computers in the network, ability to provide reports on detected software vulnerabilities and rootkits. It should be able to run scheduled, on-demand and real time on access scans.*
	•*The anti-virus solution should have automatic license deployment.*	•*The anti-virus solution should have automatic license deployment.*
	•*The anti-virus solution should have Integrated patch management functionality: centralized discovery and remote installation of OS and third-party detections and updates.*	•*The anti-virus solution should have Integrated patch management functionality: centralized discovery and remote installation of OS and third-party detections and updates.*
	•*The anti-virus solution should have centralized management of objects of backup storage and quarantine locations on all network resources in which antivirus software is installed. It should identify, quarantine, and remove viruses on infected devices without end user intervention.*	•*The anti-virus solution should have centralized management of objects of backup storage and quarantine locations on all network resources in which antivirus software is installed. It should identify, quarantine, and remove viruses on infected devices without end user intervention.*
	•*Upon end point solution installation, the centralized solution should automatically take over the client performance and ensure that it is not interfered with e.g., scans and updates run on schedule and cannot be interfered with.*	•*Upon end point solution installation, the centralized solution should automatically take over the client performance and ensure that it is not interfered with e.g., scans and updates run on schedule and cannot be interfered with.*
	•*The anti-virus solution should have centralized scanning of all network machines including new endpoints that join the network.*	•*The anti-virus solution should have centralized scanning of all network machines including new endpoints that join the network.*
	•*The anti-virus solution should have regulated updating of antivirus databases. It should also update end point policies, signatures, and engines for end points when off the network.*	•*The anti-virus solution should have regulated updating of antivirus databases. It should also update end point policies, signatures, and engines for end points when off the network.*
	•*The anti-virus solution should have technical support of the antivirus protection system and on a 24/7 basis, by telephone, email, and Internet.*	•*The anti-virus solution should have technical support of the antivirus protection system and on a 24/7 basis, by telephone, email, and Internet.*

	Threat Intelligence	***Threat Intelligence***
	•*The anti-virus solution should have Several Sources of Intelligence.*	•*The anti-virus solution should have Several Sources of Intelligence.*
	•*The anti-virus solution should have threat Intelligence services to mitigate and give actionable information of threats detected locally or globally.*	•*The anti-virus solution should have threat Intelligence services to mitigate and give actionable information of threats detected locally or globally.*
	•*The anti-virus solution should have data feeds to inform the business about risks and implications associated with cyber threats and defend against attacks even before they are launched. They may include Malicious Hash feeds, Whitelisting Data Feeds and Botnet C&C URL Feeds.*	•*The anti-virus solution should have data feeds to inform the business about risks and implications associated with cyber threats and defend against attacks even before they are launched. They may include Malicious Hash feeds, Whitelisting Data Feeds and Botnet C&C URL Feeds.*
	•*The anti-virus solution should provide a detailed inventory of applications installed on managed workstations e.g., application name, and version.*	•*The anti-virus solution should provide a detailed inventory of applications installed on managed workstations e.g., application name, and version.*
	•*The anti-virus solution should have each Data Feed give output of actionable context such as threat names, timestamps, geo-location, resolved IPs addresses of infected web resources.*	•*The anti-virus solution should have each Data Feed give output of actionable context such as threat names, timestamps, geo-location, resolved IPs addresses of infected web resources.*
	•*The anti-virus solution should have threat intelligence generated in real time.*	•*The anti-virus solution should have threat intelligence generated in real time.*
	• *The anti-virus solution should have intelligence services which allow detection of malware in all types of traffic, whether web, Email, P2P, Instant Messaging.*	• *The anti-virus solution should have intelligence services which allow detection of malware in all types of traffic, whether web, Email, P2P, Instant Messaging.*
	• *The anti-virus solution should have easy integration of actionable context into existing security solutions.*	• *The anti-virus solution should have easy integration of actionable context into existing security solutions.*
	• *The anti-virus solution should have capability to conduct intricate searches into threat indicators.*	• *The anti-virus solution should have capability to conduct intricate searches into threat indicators.*
	• *The anti-virus solution should have Advanced Persistent Threat Intelligence.*	• *The anti-virus solution should have Advanced Persistent Threat Intelligence.*
	Mitigation	***Mitigation***
	• *The anti-virus solution should have capabilities to mitigate against targeted attacks.*	• *The anti-virus solution should have capabilities to mitigate against targeted attacks.*
	• *The anti-virus solution should have capabilities to allow administrators to mitigate infections and attacks across multiple targets with minimal effort from the management console.*	• *The anti-virus solution should have capabilities to allow administrators to mitigate infections and attacks across multiple targets with minimal effort from the management console.*
	• *The anti-virus solution should have real-time ransomware protection to detect and block encryption of endpoints and shared folders.*	• *The anti-virus solution should have real-time ransomware protection to detect and block encryption of endpoints and shared folders.*
	• *The anti-virus solution should have capabilities to allow administrators to isolate individual or multiple targets from the network (micro-isolation) with minimal effort from the management console.*	• *The anti-virus solution should have capabilities to allow administrators to isolate individual or multiple targets from the network (micro-isolation) with minimal effort from the management console.*
	• *The anti-virus solution should integrate with the firewall of same brand to allow administrators to mitigate infections and attacks across multiple targets with minimal effort from the firewall.*	• *The anti-virus solution should integrate with the firewall of same brand to allow administrators to mitigate infections and attacks across multiple targets with minimal effort from the firewall.*
	• *The anti-virus solution should integrate with firewall of same brand to contain the propagation of infections and attacks across domains.*	• *The anti-virus solution should integrate with firewall of same brand to contain the propagation of infections and attacks across domains.*
	• *The anti-virus solution should allow for immediate incident response and forensic capabilities with the help of same brand firewall.*	• *The anti-virus solution should allow for immediate incident response and forensic capabilities with the help of same brand firewall.*
	Reporting & Monitoring	***Reporting & Monitoring***
	• *The anti-virus solution should have Provision of customizable endpoint compliance reports based on organizational security policies.*	• *The anti-virus solution should have Provision of customizable endpoint compliance reports based on organizational security policies.*
	• *The anti-virus solution should have Identification of notable threats for different states and different*	• *The anti-virus solution should have Identification of notable threats for different states and different*

	locations or countries.	*locations or countries.*
	• *The anti-virus solution should have proactive alerts about threats coming from botnets that target online users with the help of same brand firewall.*	• *The anti-virus solution should have proactive alerts about threats coming from botnets that target online users with the help of same brand firewall.*
	• *The solution should allow for creation of new client groups not dependent on the active directory and report on the group as well as use it in policy.*	• *The solution should allow for creation of new client groups not dependent on the active directory and report on the group as well as use it in policy.*
	Conditions:	***Conditions:***
	Vendor Responsibility	***Vendor Responsibility***
	• *Vendor must provide onsite training to ensure IT team of WVSU is capable to maintain the products*	• *Vendor must provide onsite training to ensure IT team of WVSU is capable to maintain the products*
	• *Vendor must provide 24*7 Technical support through Phone, Email, and Remote Web Assistance*	• *Vendor must provide 24*7 Technical support through Phone, Email, and Remote Web Assistance*
	• *Vendor must prepare spare parts and units in Visayas in case of hardware failure*	• *Vendor must prepare spare parts and units in Visayas in case of hardware failure*
	• *Vendor must ensure 4 hours of response time upon receiving the support call*	• *Vendor must ensure 4 hours of response time upon receiving the support call*
	• *Vendor should have engineers based in Visayas to provide onsite support if needed*	• *Vendor should have engineers based in Visayas to provide onsite support if needed*
	• *Vendor should offer quarterly health check and software upgrade to ensure products running in best condition.*	• *Vendor should offer quarterly health check and software upgrade to ensure products running in best condition.*
	• *Vendor should ensure that the configuration and implementation should be as per the requirement of the end-user*	• *Vendor should ensure that the configuration and implementation should be as per the requirement of the end-user*
	• *As part of the post qualification, the vendor must conduct a proof of concept to show that the system works with the WVSU network in accordance with the above specifications subject to the evaluation of the TWG.*	• *As part of the post qualification, the vendor must conduct a proof of concept to show that the system works with the WVSU network in accordance with the above specifications subject to the evaluation of the TWG. The firewall, authentication device and end-point security must be of the similar brand/model.*
	• *Vendor should submit a certificate of authorization from the manufacturer that they are an authorized partner or reseller to extend the maximum warranty of all equipment.*	*Vendor should submit a certificate of authorization from the manufacturer that they are an authorized partner or reseller to extend the maximum warranty of all equipment.*
	• *The vendor must present credentials for two (2) employees trained and certified as Firewall Engineers of the brand they supply.*	• *The vendor must present credentials for at least One (1) employee trained and certified as Firewall Engineers of the brand they supply. Must be an organic employee of the bidder for at least one year.*
	• *Vendor should provide a turn-over training to MIS Network Personnel for a minimum of 8hrs upon implementation of the system.*	• *Vendor should provide a turn-over training to MIS Network Personnel for a minimum of 8hrs upon implementation of the system.*
	***Documentation**:*	***Documentation**:*
	• *The manufacturer should provide a certificate of ownership of the license that the license should name WVSU as the license owner.*	• *The manufacturer should provide a certificate of ownership of the license that the license should name WVSU as the license owner.*
	• *Proper documentation and complete technology transfer are part of the requirements for the final acceptance of the project.*	• *Proper documentation and complete technology transfer are part of the requirements for the final acceptance of the project.*
	------Nothing Follows------	***------Nothing Follows------***

For guidance and information of all concerned.

JULIUS B. UNDAR
Chairperson, Bids and Awards Committee