IBA Institute of Business Administration Karachi

Leadership and Ideas for Tomorrow

Purchase Order

Approval Status: Approved

Purchase Order	Issue Date	
IBA-0000005592	05, June, 2020	
Payment Terms		**Ship Via**
30 Days		ROAD
Buyer	**Phone**	**Currency**
Purchase Department		PKR
Requestor Department		
ICT DEPARTMENT REQUESTER		

IBA Karachi
IBA MAIN CAMPUS
KARACHI
Pakistan

Supplier:
V02229
IBL UNISYS
(PVT) LTD
2ND
FLOOR,
ONE IBL
CENTER
KARACHI
Pakistan

Ship To: Store, IBA Main Campus, University Road

Bill To: Purchase Department, IBA Main Campus
University Road, Karachi
Pakistan

S. No.	Item / Description	Qty. (UOM)	Unit Price	Total Amount	Delivery Date
1	CORE SWITCH THE US$ PRICE IS CALCULATED @RS156.0, HOWEVER, ACTUAL PRICE OF US$ WILL BE CONSIDERED WHILE OPENING OF LC TENDER # IT/12/19-20 C&F BASIS SCOPE OF WORK:- US$ 44228.00 (A) CONFIGURATION, INSTALLATION AND IMPLEMENTATION WILL BE THE RESPONSIBILITY OF THE PARTNER; HOWEVER ICT OPERATION TEAM WILL BE AVAILABLE TO MAKE THE PROCESS RATIONAL. (B) PARTNER WOULD BE RESPONSIBLE TO PROVIDE THREE YEARS WARRANTY BACKED BY PRINCIPAL, SUPPORT SHOULD INCLUDE 24X7 SUPPORT DIRECT FROM PRINCIPAL EXCEPT FOR ACCESS LAYER SWITCHES APPLIED 8X5XNBD REPLACEMENT SUPPORT FACILITY IS ACCEPTABLE. (C) 24X7X4 MISSION CRITICAL DIRECT ONSITE ENGINEERING SUPPORT FOR CORE SWITCH, SERVER FORM SWITCH, INTERNET ROUTER, INTERNET FIREWALL, DC FIREWALL AND VOICE GATEWAY ROUTER (D) NBD SUPPORT FOR ACCESS LAYER SWITCH. (E) TRANSPORTATION AND LABOR INCLUSIVE (F) WARRANTY SHOULD BE FULLY BACKED BY PRINCIPAL / MANUFACTURER. BIDDER MUST SUBMIT APPROPRIATE SERVICE AGREEMENT DETAILS / APPROVAL TO	1.00 EA	6,899,568.00	6,899,568.00	30-Dec-20

Purchase Order

S. No.	Item / Description	Qty. (UOM)	Unit Price	Total Amount	Delivery Date
	GUARANTEE REQUIRED SERVICE LEVEL CORE SWITCH THE PROPOSED CORE SWITCH SHOULD INCLUDE AT LEAST 48 X 1/10 SFP+ ETHERNET L3 PORTS THE PROPOSED CORE SWITCH SHOULD INCLUDE AT LEAST 48 X 1G/10G RJ-45 COPPER ETHERNET L3 PORTS THE PROPOSED CORE SWITCH SHOULD INCLUDE AT LEAST 24 X 40G QSFP+ PORTS THE PROPOSED CORE SWITCH SHOULD HAVE AT LEAST 1 X I/O SLOTS AVAILABLE FOR FUTURE EXPANSION. THE CORE SWITCH SHOULD HAVE REDUNDANT CONTROL/SUPERVISOR CARDS WITH DEDICATED SLOTS AND SHOULD NOT USE I/O SLOTS. THE PROPOSED SWITCH SHOULD HAVE REDUNDANT AC POWER SUPPLIES (N+1). THE SWITCH SHOULD HAVE REDUNDANT SWITCH FABRICS WITH STATEFUL SWITCHOVER. SHOULD SUPPORT MAJOR LAYER 3 PROTOCOLS LIKE OSPF, BGP, IS-IS ETC. ANY LICENSE REQUIRED SHOULD BE PART OF THE PROPOSAL. THE CORE SWITCH SHALL SUPPORT SWITCHING FABRIC CAPACITY OF MINIMUM 15 TBPS & FORWARDING RATE OF MORE THAN 7 BPPS OR HIGHER. PROPOSED SWITCH SHOULD SUPPORT LINE RATE PROCESSING FOR ALL THE INTERFACES. THE CORE SWITCHES SHOULD SUPPORT MINIMUM 3 TBPS PER SLOT THE CORE SWITCH SHOULD SUPPORT SDN ARCHITECTURE WITH OPTION TO CONFIGURE THE COMPONENTS FROM CENTRALIZED SDN CONTROLLER IF REQUIRED IN FUTURE. MUST SUPPORT ADVANCED DYNAMIC ROUTING PROTOCOL AND ADVANCED QOS FEATURES THERE SHOULD NOT BE ANY HEAD OF LINE BLOCKING ARCHITECTURE TO AVOID ANY PACKET LOSS. SHOULD SUPPORT INDUSTRY STANDARDS LIKE VXLAN AND BE ABLE TO TERMINATE VXLAN FOR VLAN INTEROPERABILITY. ANY LICENSE REQUIRED FOR VXLAN SHOULD BE PART OF THE SOLUTION. THE PROPOSED SWITCH MUST SUPPORT ISSU (IN SERVICE SOFTWARE UPGRADE) THE PROPOSED SWITCH SHOULD PROVIDE NON STOP FORWARDING DURING SUPERVISOR SWITCHOVER THE SWITCH SHOULD HAVE REDUNDANT FAN TRAYS AND THE FAN TRAYS SHOULD BE				

Purchase Order

S. No.	Item / Description	Qty. (UOM)	Unit Price	Total Amount	Delivery Date
	HOT SWAPPABLE ONLINE INSERTION AND REMOVAL (OIR) OF ALL REDUNDANT COMPONENTS: SUPERVISOR, FABRIC, POWER SUPPLY, AND FAN TRAYS ETC. SHOULD SUPPORT FEATURES LIKE SPAN AND ETHANALYZERS PROPOSED HARDWARE SHOULD SUPPORT CONFIGURATION MANAGEMENT LIKE "ROLL BACK" AND ROLE BASED ACCESS CONTROL SHOULD SUPPORT STANDARD SECURITY FEATURES AND PROTOCOLS LIKE AUTHENTICATION, AUTHORIZATION, AND ACCOUNTING (AAA), SECURE SHELL (SSH) PROTOCOL VERSION 2, SIMPLE NETWORK MANAGEMENT PROTOCOL VERSION 3 (SNMPV3) SUPPORT, PORT SECURITY AND IEEE 802.1X AUTHENTICATION AND RADIUS				
2	DC FIREWALL THE FIREWALL SHOULD BE NEXT GENERATION FIREWALL THE PROPOSED BRAND MUST BE EITHER IN CHALLENGER OR LEADER MQ OF LATEST GARTNER NGFW MQ REQUIRED EITHER 8 X RJ 45 GE + 4 X SFP 1G ETHERNET PORTS OR 8 X GE COMBO ETHERNET PORTS REQUIRED NGFW + NGIPS THROUGHPUT AT LEAST 1.5 GBPS (1024B PACKET) WITH ALL FEATURES ENABLED REQUIRED MAXIMUM CONCURRENT SESSIONS AT LEAST 200,000 WITH APPLICATION VISIBILITY AND CONTROL ENABLED SHOULD SUPPORT AT LEAST 15,000 NEW CONNECTIONS PER SECOND WITH APPLICATION VISIBILITY AND CONTROL ENABLED AT LEAST 2 GBPS OF IPSEC VPN THROUGHPUT SUPPORT AT LEAST 500 SSL VPN SESSIONS. LICENSE FOR 100 SSL VPN MUST BE INCLUDED IN THE PROPOSAL. SHOULD SUPPORT LOCAL AS WELL AS CENTRALIZED MANAGEMENT AC POWER SUPPLY THE PROPOSED FIREWALLS SOLUTION SHALL BE CAPABLE OF DETECTING LINK FAILURE IN ADDITION TO DEVICE FAILURE THE PROPOSED FIREWALLS SHALL SUPPORT STANDARDS BASED LINK AGGREGATION (IEEE 802.3AD) TO ACHIEVE HIGHER BANDWIDTH NGIPS WITH FULL CONTEXTUAL AWARENESS OF USERS, INFRASTRUCTURE, APPLICATIONS, AND CONTENT TO DETECT MULTI-VECTOR THREATS REQUIRED GRANULAR APPLICATION VISIBILITY AND CONTROL WITH SUPPORT FOR MORE THAN 4,000 APPLICATIONS.	2.00 EA	343,356.00	686,712.00	30-Dec-20

Purchase Order

S. No.	Item / Description	Qty. (UOM)	Unit Price	Total Amount	Delivery Date
	REQUIRED URL FILTERING WITH SUPPORT FOR MORE THAN 120 MILLION URLS CATEGORIZED AND MORE THAN 80 URLS CATEGORIES. DETECTION OF GEO LOCATION OF IP ADDRESSES THE FIREWALL SHOULD SUPPORT SSL DECRYPTION TO ENFORCE NGIPS & NGIPS POLICIES THE FIREWALL SHOULD SUPPORT SSL DECRYPTION OF THE PUBLISHED WEB SERVERS USING THE CERTIFICATE SERVER OF THE SERVERS AND APPLYING THE LAYER 7 POLICIES THE FIREWALL SHOULD SUPPORT RATE-LIMITING TRAFFIC ON THE BASIS OF USERS, APPLICATIONS ETC. IDENTIFY AND CONTROL APPLICATIONS ON ANY PORT, NOT JUST STANDARD PORTS (INCLUDING APPLICATIONS USING HTTP OR OTHER PROTOCOLS) PROVIDE APPLICATION FUNCTION CONTROL IDENTIFY AND CONTROL APPLICATIONS SHARING THE SAME CONNECTION FINE-GRAINED VISIBILITY AND POLICY CONTROL OVER APPLICATION ACCESS / FUNCTIONALITY INTEGRATE WITH MICROSOFT ACTIVE DIRECTORY SERVER FOR IMPLEMENTING USER BASED APPLICATION ACCESS CONTROL SUPPORT CREATION OF SECURITY POLICY BASED ON AD USERS AND GROUPS IN ADDITION TO SOURCE/DESTINATION IP SUPPORT AAA, RADIUS, SNMP SUPPORT DETECTION AND PREVENTION AGAINST TUNNEL /ENCAPSULATED /ENCRYPTED ATTACKS, P2P APPLICATION RELATED THREATS PROTECT AGAINST IP AND TCP FRAGMENTATION RELATED ATTACKS SUPPORT CREATION OF USER-DEFINED APPLICATION PROTOCOL DETECTORS FILE CONTROL - DETECT AND BLOCK USERS FROM UPLOADING (SENDING) OR DOWNLOADING (RECEIVING) FILES OF SPECIFIC TYPES OVER SPECIFIC APPLICATION PROTOCOLS. THE SOLUTION MUST HAVE CONTENT AWARENESS WITH COMPREHENSIVE FILE DETECTION POLICIES AND BLOCKING OF FILES BY TYPES, PROTOCOLS AND DIRECTIONS. PROTOCOLS: FTP, HTTP, SMTP, IMAP, AND POP3 DIRECTION: UPLOAD, DOWNLOAD, BOTH FILE TYPES: OFFICE DOCUMENTS, ARCHIVE, MULTIMEDIA, EXECUTABLE, PDF ETC. AUTOMATED THREAT FEED AND IPS SIGNATURE UPDATES				

Purchase Order

S. No.	Item / Description	Qty. (UOM)	Unit Price	Total Amount	Delivery Date
	AUTOMATED THREAT CORRELATION SUPPORT POLICY CONTROL BY PORT AND PROTOCOL, APPLICATION, USER/GROUP, IP ADDRESS, IPV6 RULES/OBJECTS AND MULTICAST RULES/OBJECTS ETC. ALLOW ADMINISTRATORS TO CREATE CUSTOM IPS SIGNATURES WHEN AN IPS SIGNATURE IS MATCHED, THE FOLLOWING CONFIGURABLE ACTIONS CAN BE AUTOMATICALLY TAKEN: DETAILED ATTACK LOGGING WITH HYPERLINK TO IPS ENCYCLOPEDIA REFERENCES SNMP TRAPS PACKET LOGGING FOR FORENSIC STUDIES PASS, BLOCK OR RESET TCP SESSIONS ANALYZES FILES AT POINT OF ENTRY TO CATCH MALWARES, BLOCK MALWARES IN REAL-TIME USING ONE-TO-ONE SIGNATURE MATCHING OR MACHINE LEARNING/AI ETC. SUPPORT NETWORK TRAFFIC CLASSIFICATION APPLICATION IDENTIFICATION ACROSS ALL PORTS PROVIDE MULTIPLE MECHANISMS FOR CLASSIFYING APPLICATIONS AND APPLICATION IDENTIFICATION TECHNOLOGY BASED UPON INTRUSION PREVENTION SYSTEM (IPS) OR DEEP PACKET INSPECTION. PROVIDE THE ABILITY TO ALLOW THE ORGANIZATION TO CREATE CUSTOMIZED APPLICATION RULES HAVE SEARCHABLE LIST OF CURRENTLY IDENTIFIED APPLICATIONS ACCURATELY CLASSIFY TRAFFIC BASED ON APPLICATION (EXAMPLE: GMAIL OR FACEBOOK ETC.) BE ABLE TO CREATE FILTERS TO CONTROL GROUPS OF APPLICATION BASED ON CATEGORY, SUB CATEGORY, TECHNOLOGY, RISK OR CHARACTERISTICS ETC. SUPPORT USER-IDENTIFICATION ALLOWING AD, LDAP, RADIUS GROUPS, OR USERS TO ACCESS A PARTICULAR APPLICATION, WHILE DENYING OTHERS WEB BASED ON-BOX MANAGEMENT/GUI ADMINISTRATION PROPOSED FIREWALLS SOLUTION MUST BE CENTRALLY MANAGED FROM WEB-BASED GRAPHICAL USER INTERFACE (GUI) SNMP,SYSLOG AND NETFLOW OR EQUIVALENT THE PROPOSED FIREWALLS SHALL HAVE A REPORTING MANAGEMENT SYSTEM CAPABLE OF GENERATING REPORTS ON A MANUAL AD-HOC OR SCHEDULE (DAILY, WEEKLY, MONTHLY, ETC) BASIS. THE MANAGEMENT PLATFORM MUST INCLUDE AN INTEGRATION MECHANISM, PREFERABLY IN THE FORM OF OPEN APIS				

Purchase Order

S. No.	Item / Description	Qty. (UOM)	Unit Price	Total Amount	Delivery Date
	AND/OR STANDARD INTERFACES, TO ENABLE EVENTS AND LOG DATA TO BE SHARED WITH EXTERNAL NETWORK AND SECURITY MANAGEMENT APPLICATIONS, SUCH AS TROUBLE-TICKETING SYSTEMS, SECURITY INFORMATION AND EVENT MANAGERS (SIEMS), SYSTEMS MANAGEMENT PLATFORMS, AND LOG MANAGEMENT TOOLS. THE SOLUTION SHOULD BE ABLE TO SEND ALERT MESSAGES AT LEAST THROUGH CONSOLE ALERTING OR EMAIL MECHANISM THE MANAGEMENT PLATFORM MUST INCLUDE AN INTEGRATION MECHANISM, PREFERABLY IN THE FORM OF OPEN APIS AND/OR STANDARD INTERFACES, TO EXPORT SNMP INFORMATION TO NETWORK MANAGEMENT SYSTEMS.				
3	POE ACCESS SWITCH THE SWITCH SHOULD HAVE 48 X 1G POE+ PORTS THE SWITCH SHOULD HAVE 4 X 10G SFP UPLINK PORTS THE SWITCH SHOULD SUPPORT MORE THAN 170GBPS SWITCHING CAPACITY AND AT LEAST 130 MPPS OF FORWARDING RATE THE SWITCH SHOULD BE STACKABLE AND SHOULD SUPPORT AT LEAST 6 SWITCHES IN A STACK THE SWITCH SHOULD SUPPORT REDUNDANT POWER SUPPLY SUPPORT FOR FULL LAYER 3 ROUTING FUNCTIONALITY (RIP, OSPF, STATIC, PBR) SHOULD SUPPORT IEEE MACSEC ENCRYPTION SUPPORT FOR NETFLOW/SFLOW OR EQUIVALENT THE SWITCH SHOULD PROVIDE FEATURES SUCH AS LAYER 2, ROUTED ACCESS (RIP, OSPF), PBR, PIM STUB MULTICAST, PVLAN, QOS, 802.1X. ANY LICENSE REQUIRED SHOULD BE PART OF THE PROPOSAL FULLY MANAGED SWITCH RADIUS AND TACACS AUTHENTICATION IEEE 802.3AD LINK AGGREGATION CONTROL PROTOCOL (LACP) SUPPORT AT LEAST 512 OR HIGHER ACL RULES SNMPV3	20.00 EA	483,958.80	9,679,176.00	30-Dec-20
4	INTERNET ROUTER THE PROPOSED ROUTER SHOULD NOT BE MORE 1 RU FORM FACTOR SINCE WE HAVE LIMITED SPACE AVAILABLE IN THE RACKS SHOULD HAVE AT LEAST 2 X RJ45 GE + 2 X SFP WAN PORTS DUAL AC POWER SUPPLIES REQUIRED PROPOSED ROUTER SHOULD HAVE AT LEAST 2 INTERFACE MODULE SLOTS. PROPOSED ROUTER MUST SUPPORT A THROUGHPUT OF AT LEAST 2 GBPS OR	2.00 EA	225,576.00	451,152.00	30-Dec-20

Purchase Order

S. No.	Item / Description	Qty. (UOM)	Unit Price	Total Amount	Delivery Date
	HIGHER. THE ROUTER SHOULD SUPPORT SECURITY FEATURES SUCH AS FIREWALL, VPN, ACL, IPSEC VPN ETC. THE ROUTER SHOULD SUPPORT ENCRYPTED THROUGHPUT OF AT LEAST 500 MBPS PROPOSED ROUTERS SHOULD HAVE MULTI CORE PROCESSORS FOR HIGH SPEED WAN CONNECTIONS THE PROPOSED ROUTER SHOULD SUPPORT ADVANCED NETWORKING PROTOCOLS SUCH AS L2TPV3, BFD, MPLS, VRF, VXLAN ETC. PROPOSED ROUTER SHOULD SUPPORT FEATURES LIKE SD-WAN AND SHOULD BE ABLE TO SUPPORT SD-WAN BY SIMPLY CHANGING THE SOFTWARE SHOULD SUPPORT LAYER 3 ROUTING PROTOCOLS INCLUDING RIP, OSPF, IS-IS, BGP, PBR ETC. THE ROUTER MUST SUPPORT OVERLAY FEATURES LIKE L2TPV3 GRE MPLS SHOULD SUPPORT ONLINE INSERTION AND REMOVAL OF INTERFACE MODULES PROPOSED HARDWARE SHOULD SUPPORT QOS FEATURES LIKE CBWFQ PERFORMANCE ROUTING WRED ETC TELNET SIMPLE NETWORK MANAGEMENT PROTOCOL VERSION 3 (SNMPV3) SECURE SHELL (SSH) RADIUS AND TACACS+				
5	VOICE GATEWAY ROUTERS THE PROPOSED ROUTER SHOULD NOT BE MORE 1 RU FORM FACTOR SINCE LIMITED SPACE IS AVAILABLE IN THE RACKS SHOULD HAVE AT LEAST 2 X RJ45 GE + 2 X SFP WAN PORTS PROPOSED ROUTER SHOULD HAVE AT LEAST 3 INTERFACE MODULE SLOTS. AT LEAST 2 OF THE INTERFACE SLOTS SHOULD BE EMPTY FOR FUTURE EXPANSION PROPOSED ROUTER MUST SUPPORT A THROUGHPUT OF AT LEAST 100 MBPS OR HIGHER. THE PROPOSED ROUTER SHOULD SUPPORT UPGRADATION TO AT LEAST 2 GBPS THROUGHPUT BY SIMPLY ADDING A LICENSE WITHOUT ANY HARDWARE ADDITION. THE PROPOSED ROUTER SHOULD INCLUDE AT LEAST 4 X FXO INTERFACES PROPOSED ROUTER PROVIDE VOICE	2.00 EA	3,303,768.00	6,607,536.00	30-Dec-20

Purchase Order

S. No.	Item / Description	Qty. (UOM)	Unit Price	Total Amount	Delivery Date
	GATEWAY FUNCTIONALITY AND ANY LICENSE REQUIRED SHOULD BE PART OF THE PROPOSAL SHOULD SUPPORT AT LEAST 400 SIP/H.323 SESSIONS AND ANY LICENSE REQUIRED SHOULD BE PART OF THE PROPOSAL ROUTER SHOULD PROVIDE SIP TRUNK AND SHOULD INCLUDE LICENSES FOR AT LEAST 70 SIMULTANEOUS SIP SESSIONS. SHOULD INCLUDE AT LEAST 64 CHANNEL DSP MODULE FOR HANDLING VOICE TRAFFIC SHOULD SUPPORT FEATURES TO ACT AS CALL CONTROL FOR IP PHONES SUPPORTING AT LEAST 100 IP PHONES SHOULD SUPPORT AT LEAST 12 X E1/PRI INTERFACES TO SUPPORT DIGITAL VOICE INTERCONNECTIONS THE ROUTER SHOULD SUPPORT SECURITY FEATURES SUCH AS FIREWALL, VPN, ACL, DNS SECURITY, IPSEC, SSLVPN ETC. THE ROUTER SHOULD SUPPORT ENCRYPTED THROUGHPUT OF AT LEAST 500 MBPS PROPOSED ROUTERS SHOULD HAVE MULTI CORE PROCESSORS FOR HIGH SPEED WAN CONNECTIONS SHOULD SUPPORT SERVICE LEVEL AGREEMENTS (SLAS) FOR THE MONITORING OF THE WAN LINKS THE PROPOSED ROUTER SHOULD SUPPORT ADVANCED NETWORKING PROTOCOLS SUCH AS L2TPV3, BFD, MPLS, VRF, VXLAN ETC. THE ROUTERS SHOULD SUPPORT FEATURES LIKE APPLICATION OPTIMIZATION TO ENHANCE END USER EXPERIENCE BY HAVING SOME SORT OF CACHING ETC. IN CASE OF LOW BANDWIDTH WAN LINKS. SHOULD SUPPORT WAN OPTIMIZATION FEATURES AS BELOW: TCP FLOW OPTIMIZATION PERSISTENT LZ COMPRESSION DRE COMPRESSION APPLICATION OPTIMIZATIONS FOR FILE SHARING, EMAILS, WEB APPS, ENTERPRISE APPS ETC. PROPOSED ROUTER SHOULD SUPPORT FEATURES LIKE SD-WAN AND SHOULD BE ABLE TO SUPPORT SD-WAN BY SIMPLY CHANGING THE SOFTWARE SHOULD SUPPORT SDN. SHOULD SUPPORT NEXT GENERATION ENCRYPTION FEATURES AS BELOW. AES-128-GCM FOR AUTHENTICATED ENCRYPTION HMAC-SHA256 FOR AUTHENTICATION ECDSA-P256 FOR DIGITAL SIGNATURES SHA-256 FOR HASHING ECDH-P256 FOR KEY ESTABLISHMENT.				

Purchase Order

S. No.	Item / Description	Qty. (UOM)	Unit Price	Total Amount	Delivery Date
	SHOULD SUPPORT LAYER 3 ROUTING PROTOCOLS INCLUDING RIP, OSPF, IS-IS, BGP, PBR ETC. THE ROUTER MUST SUPPORT OVER LAY FEATURES LIKE L2TPV3 GRE MPLS SHOULD HAVE AT LEAST 4GB DRAM, WITH OPTION TO UPGRADE TO 16GB. SHOULD HAVE AT LEAST AND 4GB FLASH, WITH OPTION TO UPGRADE UP TO 16GB. SHOULD SUPPORT ONLINE INSERTION AND REMOVAL OF INTERFACE MODULES PROPOSED HARDWARE SHOULD SUPPORT QOS FEATURES LIKE: CBWFQ PERFORMANCE ROUTING WRED ETC PROPOSED ROUTER MUST COMPLY WITH FOLLOWING STANDARDS TIA-968-B CS-03 ANSI T1.101 ITU-T G.823, G.824 IEEE 802.3				
6	INTERNET FIREWALL THE FIREWALL SHOULD BE NEXT GENERATION FIREWALL THE PROPOSED BRAND MUST BE EITHER IN CHALLENGER OR LEADER MQ OF LATEST GARTNER NGFW MQ REQUIRED EITHER 8 X RJ 45 GE + 4 X SFP 1G ETHERNET PORTS OR 8 X GE COMBO ETHERNET PORTS REQUIRED NGFW + NGIPS THROUGHPUT MORE THAN 2 GBPS (1024B PACKET) WITH ALL FEATURES ENABLED REQUIRED MAXIMUM CONCURRENT SESSIONS AT LEAST 400,000 WITH APPLICATION VISIBILITY AND CONTROL ENABLED SHOULD SUPPORT MORE THAN 21,500 NEW CONNECTIONS PER SECOND WITH APPLICATION VISIBILITY AND CONTROL ENABLED MORE THAN 1 GBPS OF IPSEC VPN THROUGHPUT SHOULD SUPPORT LOCAL AS WELL AS CENTRALIZED MANAGEMENT AC POWER SUPPLY THE PROPOSED FIREWALLS SOLUTION SHALL BE CAPABLE OF DETECTING LINK FAILURE IN ADDITION TO DEVICE FAILURE THE PROPOSED FIREWALLS SHALL SUPPORT STANDARDS BASED LINK AGGREGATION (IEEE 802.3AD) TO ACHIEVE HIGHER BANDWIDTH NGIPS WITH FULL CONTEXTUAL AWARENESS OF USERS, INFRASTRUCTURE,	2.00 EA	751,920.00	1,503,840.00	30-Dec-20

Purchase Order

S. No.	Item / Description	Qty. (UOM)	Unit Price	Total Amount	Delivery Date
	APPLICATIONS, AND CONTENT TO DETECT MULTI-VECTOR THREATS REQUIRED GRANULAR APPLICATION VISIBILITY AND CONTROL WITH SUPPORT FOR MORE THAN 4,000 APPLICATIONS. REQUIRED URL FILTERING WITH SUPPORT FOR MORE THAN 120 MILLION URLS CATEGORIZED AND MORE THAN 80 URLS CATEGORIES. DETECTION OF GEO LOCATION OF IP ADDRESSES THE FIREWALL SHOULD SUPPORT SSL DECRYPTION TO ENFORCE NGIPS & NGIPS POLICIES THE FIREWALL SHOULD SUPPORT SSL DECRYPTION OF THE PUBLISHED WEB SERVERS USING THE CERTIFICATE SERVER OF THE SERVERS AND APPLYING THE LAYER 7 POLICIES THE FIREWALL SHOULD SUPPORT RATE-LIMITING TRAFFIC ON THE BASIS OF USERS, APPLICATIONS ETC. IDENTIFY AND CONTROL APPLICATIONS ON ANY PORT, NOT JUST STANDARD PORTS (INCLUDING APPLICATIONS USING HTTP OR OTHER PROTOCOLS) PROVIDE APPLICATION FUNCTION CONTROL IDENTIFY AND CONTROL APPLICATIONS SHARING THE SAME CONNECTION FINE-GRAINED VISIBILITY AND POLICY CONTROL OVER APPLICATION ACCESS / FUNCTIONALITY INTEGRATE WITH MICROSOFT ACTIVE DIRECTORY SERVER FOR IMPLEMENTING USER BASED APPLICATION ACCESS CONTROL SUPPORT CREATION OF SECURITY POLICY BASED ON AD USERS AND GROUPS IN ADDITION TO SOURCE/DESTINATION IP SUPPORT AAA, RADIUS, SNMP SUPPORT DETECTION AND PREVENTION AGAINST TUNNEL /ENCAPSULATED /ENCRYPTED ATTACKS, P2P APPLICATION RELATED THREATS PROTECT AGAINST IP AND TCP FRAGMENTATION RELATED ATTACKS SUPPORT CREATION OF USER-DEFINED APPLICATION PROTOCOL DETECTORS FILE CONTROL - DETECT AND BLOCK USERS FROM UPLOADING (SENDING) OR DOWNLOADING (RECEIVING) FILES OF SPECIFIC TYPES OVER SPECIFIC APPLICATION PROTOCOLS. THE SOLUTION MUST HAVE CONTENT AWARENESS WITH COMPREHENSIVE FILE DETECTION POLICIES AND BLOCKING OF FILES BY TYPES, PROTOCOLS AND DIRECTIONS. PROTOCOLS: FTP, HTTP, SMTP, IMAP, AND POP3				

Purchase Order

S. No.	Item / Description	Qty. (UOM)	Unit Price	Total Amount	Delivery Date
	DIRECTION: UPLOAD, DOWNLOAD, BOTH FILE TYPES: OFFICE DOCUMENTS, ARCHIVE, MULTIMEDIA, EXECUTABLE, PDF ETC. AUTOMATED THREAT FEED AND IPS SIGNATURE UPDATES AUTOMATED THREAT CORRELATION SUPPORT POLICY CONTROL BY PORT AND PROTOCOL, APPLICATION, USER/GROUP, IP ADDRESS, IPV6 RULES/OBJECTS AND MULTICAST RULES/OBJECTS ETC. ALLOW ADMINISTRATORS TO CREATE CUSTOM IPS SIGNATURES WHEN AN IPS SIGNATURE IS MATCHED, THE FOLLOWING CONFIGURABLE ACTIONS CAN BE AUTOMATICALLY TAKEN: DETAILED ATTACK LOGGING WITH HYPERLINK TO IPS ENCYCLOPEDIA REFERENCES SNMP TRAPS PACKET LOGGING FOR FORENSIC STUDIES PASS, BLOCK OR RESET TCP SESSIONS ANALYZES FILES AT POINT OF ENTRY TO CATCH MALWARES, BLOCK MALWARES IN REAL-TIME USING ONE-TO-ONE SIGNATURE MATCHING OR MACHINE LEARNING/AI ETC. SUPPORT NETWORK TRAFFIC CLASSIFICATION APPLICATION IDENTIFICATION ACROSS ALL PORTS PROVIDE MULTIPLE MECHANISMS FOR CLASSIFYING APPLICATIONS AND APPLICATION IDENTIFICATION TECHNOLOGY BASED UPON INTRUSION PREVENTION SYSTEM (IPS) OR DEEP PACKET INSPECTION. PROVIDE THE ABILITY TO ALLOW THE ORGANIZATION TO CREATE CUSTOMIZED APPLICATION RULES HAVE SEARCHABLE LIST OF CURRENTLY IDENTIFIED APPLICATIONS ACCURATELY CLASSIFY TRAFFIC BASED ON APPLICATION (EXAMPLE: GMAIL OR FACEBOOK ETC.) BE ABLE TO CREATE FILTERS TO CONTROL GROUPS OF APPLICATION BASED ON CATEGORY, SUB CATEGORY, TECHNOLOGY, RISK OR CHARACTERISTICS ETC. SUPPORT USER-IDENTIFICATION ALLOWING AD, LDAP, RADIUS GROUPS, OR USERS TO ACCESS A PARTICULAR APPLICATION, WHILE DENYING OTHERS WEB BASED ON-BOX MANAGEMENT/GUI ADMINISTRATION PROPOSED FIREWALLS SOLUTION MUST BE CENTRALLY MANAGED FROM WEB-BASED GRAPHICAL USER INTERFACE (GUI) SNMP,SYSLOG AND NETFLOW OR EQUIVALENT THE PROPOSED FIREWALLS SHALL HAVE A REPORTING MANAGEMENT SYSTEM CAPABLE OF GENERATING REPORTS ON A				

Purchase Order

S. No.	Item / Description	Qty. (UOM)	Unit Price	Total Amount	Delivery Date
	MANUAL AD-HOC OR SCHEDULE (DAILY, WEEKLY, MONTHLY, ETC) BASIS. THE MANAGEMENT PLATFORM MUST INCLUDE AN INTEGRATION MECHANISM, PREFERABLY IN THE FORM OF OPEN APIS AND/OR STANDARD INTERFACES, TO ENABLE EVENTS AND LOG DATA TO BE SHARED WITH EXTERNAL NETWORK AND SECURITY MANAGEMENT APPLICATIONS, SUCH AS TROUBLE-TICKETING SYSTEMS, SECURITY INFORMATION AND EVENT MANAGERS (SIEMS), SYSTEMS MANAGEMENT PLATFORMS, AND LOG MANAGEMENT TOOLS. THE SOLUTION SHOULD BE ABLE TO SEND ALERT MESSAGES AT LEAST THROUGH CONSOLE ALERTING OR EMAIL MECHANISM THE MANAGEMENT PLATFORM MUST INCLUDE AN INTEGRATION MECHANISM, PREFERABLY IN THE FORM OF OPEN APIS AND/OR STANDARD INTERFACES, TO EXPORT SNMP INFORMATION TO NETWORK MANAGEMENT SYSTEMS. THREE YEARS SUBSCRIPTION REQUIRED FOR ALL REQUIRED FEATURES (NGW, NGIPS, ADVANCE MALWARE PROTECTION, AND ULR FILTERING)				
7	SERVER FARM SWITCH THE PROPOSED SWITCH SHOULD HAVE 48 X 1G/10G BASE T RJ 45 PORTS. THE SWITCH SHOULD ALSO HAVE AT LEAST 4 X 40G QSFP28 PORTS ALL PORTS MUST BE LINE-RATE NON-BLOCKING SHOULD INCLUDE LAYER 3 FEATURES, INCLUDING FULL OSPF, VXLAN, AND BGP. ANY LICENSE REQUIRED SHOULD BE PART OF THE PROPOSAL THE SWITCH SHOULD SUPPORT BELOW STANDARDS IEEE 802.1Q: VLAN TAGGING IEEE 802.1S: MULTIPLE VLAN INSTANCES OF SPANNING TREE PROTOCOL IEEE 802.1D: SPANNING TREE PROTOCOL IEEE 802.1P: COS PRIORITIZATION IEEE 802.3AD: LINK AGGREGATION CONTROL PROTOCOL (LACP) IEEE 802.1W: RAPID RECONFIGURATION OF SPANNING TREE PROTOCOL IEEE 802.1AB: LLDP SHOULD HAVE DUAL REDUNDANT POWER SUPPLIES SHOULD HAVE REDUNDANT HOT SWAPPABLE FANS VALUE ADDED SERVICES: - (A) BIDDER SHOULD PROVIDE 5 DAYS TRAINING ON PROPOSED SOLUTION FOR THREE ICT PERSONS IN REGIONAL AUTHORIZED TRAINING CENTRE. (B) THE SUCCESSFUL BIDDER SHOULD	2.00 EA	1,162,746.00	2,325,492.00	30-Dec-20

Purchase Order

S. No.	Item / Description	Qty. (UOM)	Unit Price	Total Amount	Delivery Date
	ARRANGE EXECUTIVE BRIEFING SESSIONS, ENCOMPASSING ALL FEATURES AND TECHNICAL ASPECTS, FOR ICT SENIOR MANAGEMENT ON NEW TECHNOLOGY TRENDS, SMART CLASSROOMS, IOT & SDN'S AT REGIONAL HEADQUARTER OF THE PRINCIPAL / MANUFACTURER FROM THEIR MARKETING BUDGET.				
8	CENTRALIZED MANAGEMENT, MONITORING & REPORTING APPLIANCE BASED CENTRALIZED SECURITY MANAGEMENT CONSOLE AND DATABASE REPOSITORY FOR EVENT AND POLICY MANAGEMENT OF NGFW, NGIPS, AND ADVANCE MALWARE DETECTION AND PREVENTION CENTRALIZED CONFIGURATION, LOGGING, MONITORING, AND REPORTING FOR NGFW, NGIPS AND ADVANCE MALWARE DETECTION AND PREVENTION REQUIRED CENTRALIZED MANAGEMENT FOR MINIMUM 10 NGFW APPLIANCES AUTOMATICALLY AGGREGATE AND CORRELATE INFORMATION GENERATED BY NEXT GENERATION FIREWALL, NEXT GENERATION AND ADVANCE MALWARE DETECTION PROVIDE FULL STACK VISIBILITY INCLUDING THREATS USERS WEB APPLICATIONS CLIENT APPLICATIONS APPLICATION PROTOCOLS: FILE TRANSFERS MALWARE CNC SERVERS NETWORK SERVERS SERVER/HOST OPERATING SYSTEM MOBILE DEVICES VIRTUAL MACHINES ROLE-BASED DEVICE USER MANAGEMENT CUSTOMIZABLE DASHBOARD WITH CUSTOM AND/OR TEMPLATE-BASED REPORTS CORRELATION AND REMEDIATION FEATURES FOR REAL-TIME THREAT RESPONSE NETWORK BEHAVIOR AND PERFORMANCE MONITORING THE MANAGEMENT PLATFORM MUST INCLUDE AN INTEGRATION MECHANISM, PREFERABLY IN THE FORM OF OPEN APIS AND/OR STANDARD INTERFACES, TO ENABLE EVENTS AND LOG DATA TO BE SHARED WITH EXTERNAL NETWORK AND SECURITY MANAGEMENT APPLICATIONS, SUCH AS TROUBLE-TICKETING SYSTEMS, SECURITY INFORMATION AND EVENT MANAGERS (SIEMS), SYSTEMS MANAGEMENT PLATFORMS, AND LOG MANAGEMENT TOOLS.	1.00 EA	3,383,016.00	3,383,016.00	30-Dec-20

Purchase Order

S. No.	Item / Description	Qty. (UOM)	Unit Price	Total Amount	Delivery Date
			Total:	31,536,492.00	
			% GST:	Inclusive All Taxes	
			Total PO Amount:	31,536,492.00	

Amount in Words: Thirty-one million five hundred thirty-six thousand four hundred ninety-two and xx/100 Only.

Terms & Conditions:

1. Material of this order is subject to final inspection at the time of delivery.
2. We reserve the right to cancel any or all the above items if material is not in accordance with our specification or if the delivery is delayed.
3. Payment will be made through crossed cheque after the receipt of the Invoice/Bill & delivery of above item(s).
4. General Sales Tax will be paid on applicable items only.
5. Liquidity damage at the rate of 2% per month on actual will be imposed on delayed delivery.
6. The rate / item cost is final and no change what so ever will be accepted.
7. Government tax(es), levi(es) and charge(s) will be charged at actual as per SRO.
8. Competent Authority reserves the right to change / alter / remove any item or article or reduce / enhance quantity without assigning any reason.
9. Invoice/Bill to be submitted to Purchase Department.
10. Advance Payment subject to Bank Guarantee.
11. All Government taxes (including Income tax and stamp duty), levies and charges will be charged as per applicable rates / denomination of Purchase Order.
12. Stamp Duty 0.25% for Goods against total value of Purchase Order will be levied accordingly.

NOTE: *This is a computer generated Purchase Order / Work Order issued in ERP system and doesn't required signature.*