Bill of Quantity (As Single Job)

Provision of Core Network Up-gradation

S. No	Make and Model	C&F Bid Value (Foreign Currency)	Conversion Rate (Selling Rate of Exchange announced by SBP seven days prior to the opening of Bids)	Bid Value in PKR	Qty	Total Bid Value (PKR)
1	Core Switch	USD 44,228			1	
2	Server Farm Switch	USD 14,907			2	
3	POE Access Switch	USD 62,046			20	
4	Internet Router	USD 2,892			2	
5	Internet Firewall	USD 9,640			2	
	DC Firewall	USD 4,402			2	
6	Centralized Management, Monitoring & Reporting	USD 21,686			1	
7	Voice Gateway Routers	USD 42,356			2	
Total Amount C&F Value (please refer to "**instruction**" clause "g") USD 202,157/-						

Annex-A

CHAIRPERSON
CENTRAL PURCHASE COMMITTEE
INSTITUTE OF BUSINESS ADMINISTRATION
KARACHI

DR. S. M. Faisal Iradat
Assistant Professor
IBA, Karachi

MEMBER (EXTERNAL)
CENTRAL PURCHASE COMMITTEE
INSTITUTE OF BUSINESS ADMINISTRATION
KARACHI

Haris Qureshi
PPRA Advisor
IBA, Karachi

Technical specifications

S.No.	Technical specifications	Compliance (Yes\NO)
1	**Core Switch – (Qty: 1)**	
	The proposed core switch should include at least 48 x 1/10 SFP+ Ethernet L3 ports	YES
	The proposed core switch should include at least 48 x 1G/10G RJ-45 copper Ethernet L3 ports	YES
	The proposed core switch should include at least 24 x 40G QSFP+ ports	YES
	The proposed core switch should have at least 1 x I/O slots available for future expansion.	YES
	The core switch should have redundant control/supervisor cards with dedicated slots and should not use I/O slots.	YES
	The proposed switch should have redundant AC power supplies (N+1).	YES

MEMBER
CENTRAL PURCHASE COMMITTEE
INSTITUTE OF BUSINESS ADMINISTRATION

Syed Akbar Hussain Kazmi
Finance
IBA, Karachi

Institute of Business Administration ★
Office

(Pvt) Limited

2/4

	The switch should have redundant switch fabrics with stateful switchover.	Y
	Should support major layer 3 protocols like OSPF, BGP, IS-IS etc. Any license required should be part of the proposal.	Y
	The Core switch shall support switching fabric capacity of minimum 15 Tbps & forwarding rate of more than 7 bpps or higher.	Y
	Proposed switch should support line rate processing for all the interfaces.	Y
	The core switches should support minimum 3 Tbps per slot	Y
	The core switch should support SDN architecture with option to configure the components from centralized SDN controller if required in future.	Y
	Must support advanced dynamic Routing Protocol and advanced QoS features	Y
	There should not be any head of line blocking architecture to avoid any packet loss.	Y
	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.	Y
	The proposed switch must support ISSU (In Service Software Upgrade)	Y
	The proposed switch should provide Non Stop Forwarding during supervisor switchover	Y
	The switch should have redundant fan trays and the fan trays should be hot swappable	Y
	Online insertion and removal (OIR) of all redundant components: Supervisor, fabric, power supply, and fan trays etc.	Y
	Should support features like SPAN and Ethanalyzers	Y
	Proposed hardware should support configuration management like "roll back" and Role Based Access Control	Y
	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	Y
2	**(Server Farm Switch) – (Qty: 2)**	
	The proposed switch should have 48 x 1G/10G Base T RJ 45 Ports.	Yes
	The switch should also have at least 4 x 40G QSFP28 Ports	Y
	All ports must be line-rate non-blocking	Y
	Should include Layer 3 features, including full OSPF, VXLAN, and BGP. Any license required should be part of the proposal	Y
	The switch should support below standards	Y
	IEEE 802.1Q: VLAN Tagging	Y
	IEEE 802.1s: Multiple VLAN Instances of Spanning Tree Protocol	Y
	IEEE 802.1D: Spanning Tree Protocol	Y
	IEEE 802.1p: CoS Prioritization	Y
	IEEE 802.3ad: Link Aggregation Control Protocol (LACP)	Y
	IEEE 802.1w: Rapid Reconfiguration of Spanning Tree Protocol	Y

Institute of Business Administration ★ Purchase Office

(Pvt) Limited ★ IBL U

	IEEE 802.1ab: LLDP	Y
	Should have dual redundant power supplies	Y
	Should have redundant hot swappable fans	Y
	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 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.	Y
3	**PoE Access Switch (Qty: 20)**	
	The switch should have 48 x 1G PoE+ ports	Y
	The switch should have 4 x 10G SFP uplink ports	Y
	The switch should support more than 170Gbps switching capacity and at least 130 Mpps of forwarding rate	Y
	The switch should be stackable and should support at least 6 switches in a stack	Y
	The switch should support redundant power supply	Y
	Support for full layer 3 routing functionality (RIP, OSPF, Static, PBR)	Y
	Should support IEEE MacSec encryption	Y
	Support for NetFlow/Sflow or equivalent	Y
	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	Y
	Fully managed switch	Y
	RADIUS and TACACS authentication	Y
	IEEE 802.3ad Link Aggregation Control Protocol (LACP)	Y
	Support at least 512 or higher ACL rules	Y
	SNMPv3	Y
4	**Internet Router – (Qty: 2)**	
	The proposed router should not be more 1 RU form factor since we have limited space available in the racks	Y
	Should have at least 2 x RJ45 GE + 2 x SFP WAN ports	Y
	Dual AC power supplies required	Y
	Proposed router should have at least 2 interface module Slots.	Y
	Proposed router must support a throughput of at least 2 Gbps or higher.	Y
	The router should support security features such as Firewall, VPN, ACL, IPSEC VPN etc.	Y
	The Router should support encrypted throughput of at least 500 Mbps	Y
	Proposed routers should have multi core processors for high speed WAN Connections	Y

Institute of Bus[illegible] ★ [illegible]tion
Purchase Office

	The proposed router should support advanced networking protocols such as L2TPv3, BFD, MPLS, VRF, VXLAN etc.	Y
	Proposed router should support features like SD-WAN and should be able to support SD-WAN by simply changing the software	Y
	Should support Layer 3 routing protocols including RIP, OSPF, IS-IS, BGP, PBR etc.	Y
	The router must support Overlay features like	Y
	L2TPv3	Y
	GRE	Y
	MPLS	Y
	Should support Online Insertion and Removal of interface modules	Y
	Proposed hardware should support QoS features like	Y
	CBWFQ	Y
	Performance Routing	Y
	WRED etc	Y
	Telnet	Y
	Simple Network Management Protocol Version 3 (SNMPv3)	Y
	Secure Shell (SSH)	Y
	RADIUS and TACACS+	Y
5	**Internet Firewall (Qty: 2)**	
	The firewall should be Next Generation Firewall	Y
	The proposed brand must be either in Challenger or Leader MQ of latest Gartner NGFW MQ	Y
	Required either 8 x RJ 45 GE + 4 x SFP 1G Ethernet ports or 8 x GE Combo Ethernet ports	Y
	Required NGFW + NGIPS throughput more than 2 Gbps (1024B Packet) with all features enabled	Y
	Required maximum concurrent sessions at least 400,000 with Application Visibility and Control enabled	Y
	Should support more than 21,500 new connections per second with Application Visibility and Control enabled	Y
	More than 1 Gbps of IPSEC VPN throughput	Y
	Should support local as well as centralized management	Y
	AC power supply	Y
	The proposed firewalls solution shall be capable of detecting link failure in addition to device failure	Y
	The proposed firewalls shall support standards based link aggregation (IEEE 802.3ad) to achieve higher bandwidth	Y
	NGIPS with full contextual awareness of users, infrastructure, applications, and content to detect multi-vector threats	Y
	Required granular Application Visibility and Control with support for more than 4,000 applications.	Y

Institute of Business Administration ★ [illegible] Office

IB[illegible]sys[illegible] ★ Limited

	Required URL Filtering with support for more than 120 Million URLs categorized and more than 80 URLs categories.	y
	Detection of Geo location of IP Addresses	y
	The firewall should support SSL decryption to enforce NGIPS & NGIPS policies	y
	The firewall should support SSL decryption of the published web servers using the certificate server of the servers and applying the layer 7 policies	y
	The firewall should support rate-limiting traffic on the basis of users, applications etc.	y
	Identify and control applications on any port, not just standard ports (including applications using HTTP or other protocols)	y
	Provide application function control	y
	Identify and control applications sharing the same connection	y
	Fine-grained visibility and policy control over application access / functionality	y
	Integrate with Microsoft Active Directory Server for implementing user based application access control	y
	Support creation of security policy based on AD Users and Groups in addition to source/destination IP	y
	Support AAA, RADIUS, SNMP	y
	Support detection and prevention against tunnel /encapsulated /encrypted attacks, p2p application related threats	y
	Protect against IP and TCP fragmentation related attacks	y
	Support creation of user-defined application protocol detectors	y
	File control - detect and block users from uploading (sending) or downloading (receiving) files of specific types over specific application protocols.	y
	The solution must have content awareness with comprehensive file detection policies and blocking of files by types, protocols and directions.	y
	Protocols: FTP, HTTP, SMTP, IMAP, and POP3	y
	Direction: Upload, Download, Both	y
	File Types: Office Documents, Archive, Multimedia, Executable, PDF etc.	y
	Automated threat feed and IPS signature updates	y
	Automated threat correlation	y
	Support policy control by port and protocol, application, user/group, IP address, IPV6 rules/objects and multicast rules/objects etc.	y
	Allow administrators to create custom IPS signatures	y
	When an IPS signature is matched, the following configurable actions can be automatically taken:	y
	Detailed attack logging with hyperlink to IPS encyclopedia references	y
	SNMP traps	y
	Packet logging for forensic studies	y
	Pass, block or reset TCP sessions	y

	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.	Y
	Support network traffic classification application identification across all ports	Y
	Provide multiple mechanisms for classifying applications and application identification technology based upon Intrusion Prevention System (IPS) or deep packet inspection.	Y
	Provide the ability to allow the organization to create customized application rules	Y
	Have searchable list of currently identified applications	Y
	Accurately classify traffic based on application (example: Gmail or Facebook etc.)	Y
	Be able to create filters to control groups of application based on category, sub category, technology, risk or characteristics etc.	Y
	Support user-identification allowing AD, LDAP, RADIUS groups, or users to access a particular application, while denying others	Y
	Web based on-box Management/GUI administration	Y
	Proposed Firewalls solution must be centrally managed from Web-Based Graphical User Interface (GUI)	Y
	SNMP,SYSLOG and Netflow or equivalent	Y
	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.	Y
	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.	Y
	The solution should be able to send alert messages at least through Console Alerting or Email mechanism	Y
	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.	Y
	Three Years Subscription required for all required features (NGW, NGIPS, Advance Malware Protection, and ULR Filtering)	Y
6	**DC Firewall (Qty: 2)**	
	The firewall should be Next Generation Firewall	Y
	The proposed brand must be either in Challenger or Leader MQ of latest Gartner NGFW MQ	Y
	Required either 8 x RJ 45 GE + 4 x SFP 1G Ethernet ports or 8 x GE Combo Ethernet ports	Y

	Required NGFW + NGIPS throughput at least 1.5 Gbps (1024B Packet) with all features enabled	Y
	Required maximum concurrent sessions at least 200,000 with Application Visibility and Control enabled	Y
	Should support at least 15,000 new connections per second with Application Visibility and Control enabled	Y
	At least 2 Gbps of IPSEC VPN throughput	Y
	Support at least 500 SSL VPN sessions.	Y
	License for 100 SSL VPN must be included in the proposal.	Y
	Should support local as well as centralized management	Y
	AC power supply	Y
	The proposed firewalls solution shall be capable of detecting link failure in addition to device failure	Y
	The proposed firewalls shall support standards based link aggregation (IEEE 802.3ad) to achieve higher bandwidth	Y
	NGIPS with full contextual awareness of users, infrastructure, applications, and content to detect multi-vector threats	Y
	Required granular Application Visibility and Control with support for more than 4,000 applications.	Y
	Required URL Filtering with support for more than 120 Million URLs categorized and more than 80 URLs categories.	Y
	Detection of Geo location of IP Addresses	Y
	The firewall should support SSL decryption to enforce NGIPS & NGIPS policies	Y
	The firewall should support SSL decryption of the published web servers using the certificate server of the servers and applying the layer 7 policies	Y
	The firewall should support rate-limiting traffic on the basis of users, applications etc.	Y
	Identify and control applications on any port, not just standard ports (including applications using HTTP or other protocols)	Y
	Provide application function control	Y
	Identify and control applications sharing the same connection	Y
	Fine-grained visibility and policy control over application access / functionality	Y
	Integrate with Microsoft Active Directory Server for implementing user based application access control	Y
	Support creation of security policy based on AD Users and Groups in addition to source/destination IP	Y
	Support AAA, RADIUS, SNMP	Y
	Support detection and prevention against tunnel /encapsulated /encrypted attacks, p2p application related threats	Y
	Protect against IP and TCP fragmentation related attacks	Y
	Support creation of user-defined application protocol detectors	Y

Institute of Business Administration ★ Office

SYS (Pvt) Limited

	File control - detect and block users from uploading (sending) or downloading (receiving) files of specific types over specific application protocols.	Y
	The solution must have content awareness with comprehensive file detection policies and blocking of files by types, protocols and directions.	Y
	Protocols: FTP, HTTP, SMTP, IMAP, and POP3	Y
	Direction: Upload, Download, Both	Y
	File Types: Office Documents, Archive, Multimedia, Executable, PDF etc.	Y
	Automated threat feed and IPS signature updates	Y
	Automated threat correlation	Y
	Support policy control by port and protocol, application, user/group, IP address, IPV6 rules/objects and multicast rules/objects etc.	Y
	Allow administrators to create custom IPS signatures	Y
	When an IPS signature is matched, the following configurable actions can be automatically taken:	Y
	Detailed attack logging with hyperlink to IPS encyclopedia references	Y
	SNMP traps	Y
	Packet logging for forensic studies	Y
	Pass, block or reset TCP sessions	Y
	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.	Y
	Support network traffic classification application identification across all ports	Y
	Provide multiple mechanisms for classifying applications and application identification technology based upon Intrusion Prevention System (IPS) or deep packet inspection.	Y
	Provide the ability to allow the organization to create customized application rules	Y
	Have searchable list of currently identified applications	Y
	Accurately classify traffic based on application (example: Gmail or Facebook etc.)	Y
	Be able to create filters to control groups of application based on category, sub category, technology, risk or characteristics etc.	Y
	Support user-identification allowing AD, LDAP, RADIUS groups, or users to access a particular application, while denying others	Y
	Web based on-box Management/GUI administration	Y
	Proposed Firewalls solution must be centrally managed from Web-Based Graphical User Interface (GUI)	Y
	SNMP,SYSLOG and Netflow or equivalent	Y
	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.	Y

IBL UNISYS (Pvt) Limited

Institute of Business Administration
Office

	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.	Y
	The solution should be able to send alert messages at least through Console Alerting or Email mechanism	Y
	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.	Y
7	**Centralized Management, Monitoring & Reporting: (Qty: 1)**	
	Appliance based Centralized security management console and database repository for event and policy management of NGFW, NGIPS, and Advance Malware Detection and Prevention	Y
	Centralized configuration, logging, monitoring, and reporting for NGFW, NGIPS and Advance Malware Detection and Prevention	Y
	Required Centralized Management for Minimum 10 NGFW Appliances	Y
	Automatically aggregate and correlate information generated by Next Generation Firewall, Next Generation and Advance Malware Detection	Y
	Provide full stack visibility including	Y
	Threats	Y
	Users	Y
	Web Applications	Y
	Client applications	Y
	Application protocols:	Y
	File transfers	Y
	Malware	Y
	CNC servers	Y
	Network servers	Y
	Server/host operating system	Y
	Mobile devices	Y
	Virtual machines	Y
	Role-based device user management	Y
	Customizable dashboard with custom and/or template-based reports	Y
	Correlation and remediation features for real-time threat response	Y
	Network behavior and performance monitoring	Y
	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.	Y

8	**Voice Gateway Router : (QTY:2)**	
	The proposed router should not be more 1 RU form factor since limited space is available in the racks	Y
	Should have at least 2 x RJ45 GE + 2 x SFP WAN ports	Y
	Proposed router should have at least 3 interface module Slots.	Y
	At least 2 of the interface slots should be empty for future expansion	Y
	Proposed router must support a throughput of at least 100 Mbps or higher.	Y
	The proposed router should support upgradation to at least 2 Gbps throughput by simply adding a license without any hardware addition.	Y
	The proposed router should include at least 4 x FXO interfaces	Y
	Proposed router provide voice gateway functionality and any license required should be part of the proposal	Y
	Should support at least 400 SIP/H.323 Sessions and any license required should be part of the proposal	Y
	Router should provide SIP trunk and should include licenses for at least 70 simultaneous SIP Sessions.	Y
	Should include at least 64 channel DSP module for handling voice traffic	Y
	Should support features to act as Call Control for IP Phones supporting at least 100 IP Phones	Y
	Should support at least 12 x E1/PRI Interfaces to support digital voice interconnections	Y
	The router should support security features such as Firewall, VPN, ACL, DNS Security, IPSEC, SSLVPN etc.	Y
	The Router Should support encrypted throughput of at least 500 Mbps	Y
	Proposed routers should have multi core processors for high speed WAN Connections	Y
	Should support Service Level Agreements (SLAs) for the monitoring of the WAN links	Y
	The proposed router should support advanced networking protocols such as L2TPv3, BFD, MPLS, VRF, VXLAN etc.	Y
	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.	Y
	Should support WAN optimization features as below:	Y
	TCP Flow Optimization	Y
	Persistent LZ Compression	Y
	DRE Compression	Y
	Application Optimizations for file sharing, emails, web apps, enterprise apps etc.	Y
	Proposed router should support features like SD-WAN and should be able to support SD-WAN by simply changing the software	Y
	Should support SDN.	Y
	Should support Next Generation Encryption features as below.	Y

	AES-128-GCM for Authenticated Encryption	Y
	HMAC-SHA256 for Authentication	Y
	ECDSA-P256 for Digital Signatures	Y
	SHA-256 for Hashing	Y
	ECDH-P256 for Key Establishment.	Y
	Should support Layer 3 routing protocols including RIP, OSPF, IS-IS, BGP, PBR etc.	Y
	The router must support Over lay features like	Y
	L2TPv3	Y
	GRE	Y
	MPLS	Y
	Should have at least 4GB DRAM, with option to upgrade to 16GB.	Y
	Should have at least and 4GB Flash, with option to upgrade up to 16GB.	Y
	Should support Online Insertion and Removal of interface modules	Y
	Proposed hardware should support QoS features like:	Y
	CBWFQ	Y
	Performance Routing	Y
	WRED etc	Y
	Proposed router must comply with following standards	Y
	TIA-968-B	Y
	CS-03	Y
	ANSI T1.101	Y
	ITU-T G.823, G.824	Y
	IEEE 802.3	Y

Scope of Work:-

(c) Configuration, installation and implementation will be the responsibility of the Partner; however ICT Operation Team will be available to make the process rational.

(d) 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.

(e) 24x7x4 Mission Critical Direct onsite engineering support for Core Switch, Server form switch, Internet Router, Internet Firewall, DC Firewall and Voice gateway router

(f) NBD Support for access layer switch.

(g) Transportation and labor inclusive

(h) Warranty should be fully backed by principal / manufacturer. Bidder must submit appropriate service agreement details / approval to guarantee required service level

IBL U... Limited

Stamp & Signature

Institute of Business Administration ★ Purchase Office

Principal Criteria

a) Principal should have local presence in Pakistan
b) Principal should have local depot facility for instant RMA and should have the mechanism to provide replacement in Karachi as per the SLA matrix of acquired products.
c) Principal should have local onsite resources
d) Principal should have network deployments in five public sector universities of Pakistan.

Total Amount (C&F Foreign Currency)	USD 202,157/-

Total Amount* C&F Foreign Currency *(in words) US Dollar Two Hundred & Two thousand, One undred fifty Seven Only.

To be filled by IBA, Karachi (as per clause 4(a))

Total Amount PKR (in words) ________________________________

MEMBER (EXTERNAL)
CENTRAL PURCHASE COMMITTEE
INSTITUTE OF BUSINESS ADMINISTRATION
KARACHI

Haris Qureshi
PPRA Advisor
HCJ

CHAIRPERSON
CENTRAL PURCHASE COMMITTEE
INSTITUTE OF BUSINESS ADMINISTRATION
KARACHI

DR S.M. Faisal Iradat
Assistant Professor
IBA, Karachi

MEMBER
CENTRAL PURCHASE COMMITTEE
INSTITUTE OF BUSINESS ADMINISTRATION
KARACHI

Syed Akbar Hussain Kazmi
Finance
IBA, Karachi

IBL UNISYS (PVT) Limited

Stamp & Signature

Institute of Business Administration
Purchase Office