



Business Finance for the Poor in Bangladesh (BFP-B)
Terms of Reference for Procurement of Server, Firewalls etc.
For Microfinance Credit Information Bureau (MF CIB)

Background:

Business Finance for the Poor in Bangladesh (BFP-B) is a seven year programme funded by UK aid from the UK government. The Bangladesh Bank (BB), the central bank of Bangladesh, and Microfinance Regulatory Authority [MRA] are the implementing agency, and the Financial Institutions Division (FID) of the Ministry of Finance (MoF), Government of Bangladesh (GoB), is the executing agency. Nathan Associates London Ltd. is appointed as the management agency for the programme. The programme aims to promote innovative finance and financial services for micro and small enterprises (MSEs) in the country. It is designed to couple of social and economic welfare objectives with a commercially-sound approach to increase access to finance for MSEs, especially those that are currently underserved by the formal financial sector. BFP-B has three components: Challenge Fund, Microfinance Credit Information Bureau (MF- CIB), and Policy. The Challenge Fund has been catalysing and supporting innovative financing products and delivery channels to foster financial inclusion; the MF- CIB will assist Microfinance Institutions (MFIs) and banks to reduce systematic risks through its establishment; and the Policy Component has been working as a support function for these two components and focusing on facilitating a collaborative approach to financial sector policy and regulatory reform to create an enabling regulatory environment for the MSE sector in Bangladesh and increasing financial inclusion for small business.

Objective of the Services

BFP-B aims to improve the credit worthiness of small businesses, which will enable financial institutions to reduce the cost of risk assessment and improve the risk-adjusted returns of lending and investing in small businesses.

The CIB component of BFP-B is assisting the Microcredit Regulatory Authority to establish a functioning microfinance credit information bureau (MF-CIB).

Under the component Microfinance Credit Information Bureau (MF- CIB) following **Server, Firewalls and End Point Security** products to be procured and supplied for smooth functioning of microfinance credit information bureau (MF-CIB).

List of Products (hardware and software) to be procured;

Serial	Item Name	Brief Description	Qty –Nos/lot

1	Server	Chassis: 2U Rack Mountable Rail kit Processor: 2XIntel Xeon-Silver 4214 (2.2 GHz/12-core/85W) (2 Nos Processor) Core per Processor: 12 (Twelve) Core	3 Nos.
2	SAN Switch	Rack Mountable Full duplex switch should support 24 ports with 8/16 Gbps FC connectivity with 12 active ports	2 Nos.
3	Rack Including KVM, Basic PDU and ATS	Same Brand as Server Height: 42U Width 19" PDU brand same as Rack Brand Capacity: 16 Amp.	1 No.
4	SAN Storage	Storage Controller: Storage system should a unified system supporting all block and file protocols scaling to at 12 controllers (6 HA Pairs)	1 No.
5	Next Generation Firewalls with HA	Rack Mountable	2 Nos.
6.	Email Security	As mentioned in details Specification	Lot
7.	End Point Security -Client Server Based Antivirus	As mentioned in details specifications	50 Users lot

(Details technical specification of each item in Attachment- A)

Vendor/Supplier Eligibility:

1. Minimum 5 years experience in IT/Office equipment business
2. Dealer/Importer/Manufacturer/Supplier are eligible for participating in the bidding process
3. Supplier/vendor must have valid Trade licence, TIN and VAT Reg. and other membership/certification if any
4. Have previous experience of large corporate supply of similar items
5. Supplier/Vendor should have local office/agent/representative with adequate after sales services facilities

(Please provide details where necessary with documentary proofs in favour of each of the above items)

Other Terms:

1. Sealed quotation is requested for all items (divided in 2 Lots) from each supplier. Vendor/Supplier may submit for any single Lot (as mentioned in the details specification) partial quotation.

2. Vendor/Supplier is requested to submit their quotation both **Technical and Financial** in prescribed form as **Attachment –A and Attachment-B** given below
3. Sealed quotation to be dropped in the tender box at **Level -3, House # 71, Road # 27, Gulshan-1, Dhaka by 3:00 pm 27th October 2019**
4. Successful vendor is to accomplish with the supply of required equipment within maximum **80 (eighty) days** from the date of contract award and sign off.
5. Goods to be delivered and installed at MF-CIB office at Moghbazar, Dhaka
6. Quotation price of the each item to be mentioned in **both BD Taka and GBP** with current exchange rate and at least 30 days validity.
7. Quoted price should be inclusive of VAT and any other taxes
8. Contract to be awarded to the successful vendor by **Nathan Associates London Ltd.**
9. Single payment will be made after successful delivery of goods as per contract/work order
10. Supplier will receive their payment in GBP through direct bank transfer in the supplier's designated bank account in Bangladesh
11. Business Finance for the Poor in Bangladesh (BFP-B) program office at Dhaka reserve right to accept or reject any quotation

(For further information Please contact Md Aminur Rahman, mobile 01711 810065)

End

Attachment - A



Business Finance for the Poor in Bangladesh (BFP-B)
Technical Specification of the Bidders Offer

Lot-1: Server, Storage, SAN Switch, Rack

1. Server Specification: Qty. 03

Description	Technical Specifications	Bidder Response
Brand Name	HP/DELL/Any Other Reputed Brand	
Model	To be mentioned by the bidder	
Country of origin	USA	
Chassis	2U Rack Mountable Rail Kit	
Processor	2 x Intel Xeon-Silver 4214 (2.2GHz/12-core/85W) Processor	
Number of Processor	02 (Two)	
Chipset	Intel C620 Chipset or higher	
Core per Processor	Minimum 12 (Twelve) core	
Cache Memory per processor	Integrated 16.5 MB	
Memory	<ul style="list-style-type: none"> 64 GB (4 x 16GB x4 DDR4-2666 advanced ECC capability Min. 24 DIMM slots per server 	
Graphics	<ul style="list-style-type: none"> Integrated 16 MB or higher Video Memory 32 MB Flash System Management Memory 	
Hard Drive	<ul style="list-style-type: none"> 5x 1.2 TB SAS 12G 10K SFF (2.5in) SFF Hard Disk slot expandability up to 16 drives 	
DVD+/RW	<ul style="list-style-type: none"> Factory integrated DVD+/RW optical media kit 	
Storage Array Controller:	<ul style="list-style-type: none"> Hardware RAID Controller with 4 GB flash backed write cache support RAID 0, 1, 5, 6, 10, 50, 60, 1 ADM, 10 ADM (Advanced Data Mirroring) FIPS 140-2 Cryptographic Module Validation DRAM ECC detects and corrects data bit errors features 	
Expansion slots and I/O	<ul style="list-style-type: none"> Up to Six (6) PCIe 3.0 I/O expansion Slots 1 x optional Serial, up to 2 Video, 1 x Remote management port, Min 1 Micro SD slot, up to 5 USB 3.0 Ports 	
Network Interface Controller	<ul style="list-style-type: none"> 2x1Gb and 2x10 Gb, 4-port Ethernet adapter LOM 	
HBA	<ul style="list-style-type: none"> 2x16Gb FC HBA 	
Remote management port & features	Integrated remote management capability from day 1 with dedicated network connection supporting GUI. <ul style="list-style-type: none"> Remote console 	

	<ul style="list-style-type: none"> Intelligent system tuning 	
Power Supply & System Fan Support	Minimum 2x 750W (or higher) standard redundant power supply & Hot Plug Fans with N+1 redundancy	
Operating System Support N.B : Licensed Windows server 2019 for 1 server	<ul style="list-style-type: none"> Operating Systems and Virtualization Software Windows Server 2012 R2 Windows Server 2016 Windows Server 2019 VMware ESXi 6.0 U3 VMware ESXi 6.5, 6.7 and U1 upon release Red Hat Enterprise Linux (RHEL) 6.9 and 7.3 SUSE Linux Enterprise Server (SLES) 11 SP4 and 12 SP2 CentOS Canonical Ubuntu 	
The Payment Card Industry Data Security Standard (PCI DSS) Compliance	<ul style="list-style-type: none"> The Server should be Payment Card Industry Data Security Standard (PCI DSS) complaint to protect the safety of credit, debit, and cash card transactions and protect cardholders against misuse of their personal information. 	
Industry Standard Compliance	<ul style="list-style-type: none"> ACPI 6.1 Compliant PCIe 3.0 Compliant WOL Support Microsoft® Logo certifications PXE Support USB 3.0 Compliant (internal); USB 2.0 Compliant (external ports via SUV) SMBIOS 3.1 UEFI 2.6 Redfish API Secure Digital 2.0 Triple Data Encryption Standard (3DES) 	
Warranty	Proposed Server must have 5 (Five) years full 24x7 support warranty with parts Replacement supporting back to back OEM Warranty. 24x7 support can be checked through OEM website.	

2. SAN-Storage Specification Qty. 01

SL	Item	Description	Bidder's Offer
01	Type	Storage	
02	Brand	International reputed Brand.	
03	Model	To be mentioned by the Bidder.	
04	Processor	Min. 2 X Intel 6 Core Processor.	
05	Architecture	Proposed Storage System should be natively Unified Storage System (File and Block)	

SL	Item	Description	Bidder's Offer
		having Active-Active Controllers (No Additional Controllers/Headers for NAS/SAN).	
06	Availability	Proposed Storage System should have 99.999% availability with no single point of failure.	
07	Storage DRAM Cache	The storage controllers & operating environment should natively support enhanced caching technologies, Storage system should have minimum 2 or 4 controllers with minimum 48 GB Cache or Higher. Storage Cache should be scalable up to at least 800 GB.	
08	Data Protection	Proposed system should have data protection designed for SSD, SATA and SAS drives. Data Protection should be configured to sustain disk failure in any single data protection group	
09	Storage Capacity	The solution shall ensure movement of entire volume/LUN as a whole non-disruptively between the nodes to optimize the system for capacity utilization and performance. This feature shall also be used for seamless hardware upgrades i.e., there should be no downtime for the Server / Host / User during this movement of entire LUN / Volume.	
		The storage shall support SAS, SSD and SATA based disks simultaneously. The storage should be designed in such a way so as to provide dedicated RAID storage groups for each controller, which should allow any 2 drive failure protection at any given point in time. The storage should provide at least 20 TB of usable space.	
		Proposed storage system should have intelligent data tiring to move data across SSD, SAS and NL-SAS within single pool. Proposed system should also support SSD drives to be used as cache.	
		The system should support RAID 1, 4, 5, RAID1+0, RAID6 or equivalent. The RAID implementation on the storage will be such that it is able to protect against two drive failing in the same RAID Group simultaneously. It should be possible to assign multiple raid arrays to single pool and it should be possible to define a volume which spans across all the disks in the pool.	
10	OS support	Support for industry-leading Operating System platforms including: LINUX , Microsoft Windows, HP-UX, SUN Solaris, IBM-AIX, etc. It shall support connecting hosts over and iSCSI and shall be supplied with any Multipathing software if required with the solution.	
11	Protocol Support	Storage system should natively support standard protocol such as Block Access (FC	

SL	Item	Description	Bidder's Offer
		and iSCSI) and File Access Protocols (CIFS, NFS),SMB, FTP, Protocols on Single Storage Pool.	
I 2	Connectivity	Proposed solution should support minimum 2 ×10 Gb/ iSCSI ports for NAS operations ; minimum 2×10GbE Optical ports , minimum 2 ×16Gbps FC ports per controller which should be backward compatible to 8Gbps across Dual Controllers, 4×6Gbps Wide SAS 2.0 ports across dual controllers All these ports with licenses should be provided from day one.	
13	Application Integration	Proposed solution should support integration with industry leading applications/database for creating application-consistent repurpose and protection copies of data. Application integration should be managed from separate software from storage management software for better management and should support RBAC.	
14	Snapshots	Proposed storage should have Redirect-on-Write (ROW) based snapshots with ability to create snapshots up to 10 levels and any-to-any snapshot restoration. Each snapshot should support both Read and Read-Write access and should also support replication	
15	Data Encryption	Proposed Storage should support 256-bit AES Data at Rest Encryption.	
16	Data Replication	The solution should support Sync and Asynchronous replication for the full supported capacity of the system for all the protocols specified above. The solution shall support replication in cascade, one to many and manyto-one mode. The replication solution on storage shall support failover to DR storage and failback as and when required. The failover to the DR site shall be controlled from the Storage management GUI and should include the functionality to execute any custom post-processing scripts to make sure the complete process is automated. It should be possible to test the DR operations without interrupting the replication relationship.	
17	High Availability	The storage system must be configured to continuously serve data in event of any controller failure. System should offer capability for 2 disks and 3 disks data parity protection and failure of any 2 disks or 3 disks.	
18	De- Duplication and Compression	Proposed storage system should support both inline and post process data de-duplication and compression for all kinds of structured and unstructured data on both block and file.	
19	Management	Proposed storage should have enterprise class HTML5 GUI, Proposed system should	

SL	Item	Description	Bidder's Offer
		also offer SaaS based storage analytics and monitoring tool with ability to store historical logs for trend analysis.	
20	Cloud Integration	Proposed storage should have native cloud integration for archiving data and recall data to (and from) cloud.	
21	Licensing	Proposed storage should have all-inclusive licensing for entire capacity for all storage features.	
22	Continuous Data Protection with Replication.	Proposed solution should support block-level replication on local as well as remote SAN Array. Proposed solution also should support continuous data protection feature with ability to create and configured multiple check-points for restore for every data change locally as well as on remote SAN array. Proposed system should support different retention of check points on local and remote array.	
23	Bandwidth Optimization	Proposed solution should support bandwidth optimization features for reducing WAN bandwidth requirement (de-duplication, compression, etc.). Bidders not having native bandwidth optimization features should include additional WAN optimization device.	
24	Application Consistency	Proposed solution should support creating group of LUNs as single replication group for data consistency. Solution should have feature to ensure recovery consistency for single application or inter-dependent applications. Proposed storage solution should provide licenses for creating application integrated copies and application consistent disaster recovery (DR).	
25	Role Based Access (RBAC)	Proposed solution should support RBAC and integration with authentication servers (Active directory)	
26	Dial Home Support	Proposed solution should support dial home notification feature for proactive case logging. Dial home data should be accessible to IT team.	
27	Form Factor	Rack mountable with Rail Kit including front side bezel and accessories.	
28	Warranty	Five (5) years proactive support and parts replication services direct from the OEM. The OEM should have own parts exchange center /ware-house within Dhaka city. OEM also should have local office in Bangladesh for the urgent support.	
29	Training	The vendor must provide adequate and appropriate training to at least 2 (Two) personnel for efficient operation of the Security system at OEM Regional Location for minimum 5 days with all expenses.	

3.SAN Switch Qty. 02

SL No.	Parameters	Description	Bidder Response
1	Quantity	02 (Two)	
2	Quality Certification	ISO/FCC/UL/CE or To be mentioned by the bidder	
3	Model	To be mentioned by the bidder	
4	Country of Origin	To be mentioned by the bidder	
5	Country of Assemble /Manufacture	To be mentioned by the bidder	
6	Specification	Full duplex switch should support 24 ports with 8/16 Gbps FC connectivity where 12 active ports with 8/16 Gbps SFP.	
7	Connectivity speed	8/16 GBPS Supported with above storage units and auto negotiable	
8	Port Options	The switch shall support different port types such as FL_Port, F_Port and E_Port; self-discovery based on switch type (U_Port); optional port type control in Access Gateway mode: F_Port and NPIV-enabled N_Port.	
9	Rack Mountable	The switch should be rack mountable	
10	firmware Upgrades	Non-disruptive Microcode/ firmware Upgrades and hot code activation.	
11	Aggregate bandwidth	The switch shall provide preferable Aggregate bandwidth of 384 Gbit/sec: 12 ports × 16 Gbit/sec (data rate) end to end.	
12	Switch Management software	Switch shall have support for web based management and should also support CLI.	
13	USB Port Option	The switch should have USB port for firmware download, support save, and configuration upload/download.	
14	Power Efficiency	Offered SAN switches shall be highly efficient in power consumption.	
15	Self-Diagnostics	Switch shall support POST and online/offline diagnostics, including RAS trace logging, environmental monitoring, non-disruptive daemon restart, FC ping and Path info (FC trace route), port mirroring (SPAN port).	
16	Quality of Service	Offered SAN switch shall support services such as Quality of Service (QoS) to help optimize application performance in consolidated, virtual environments. It should be possible to define high, medium and low	

		priority QoS zones to expedite high-priority traffic.	
17	Switch port intelligence	SAN switch shall support to restrict data flow from less critical hosts at preset bandwidths.	
18	Zoning Feature	It should be possible to isolate the high bandwidth data flows traffic to specific ISLs by using simple zoning	
19	ISL Trunking	The Switch should be configured with the Zoning and shall support ISL Trunking features when cascading more than 2 numbers of SAN switches into a single fabric. The switch shall be able to support ISL trunk up to 64 Gbit/sec between a pair of switches for optimal bandwidth utilization and load balancing.	
20	Bandwidth Management	Offered SAN switches shall support to measure the top bandwidth consuming traffic in real time for a specific port or a fabric which should detail the physical or virtual device.	
21	Common Feature	Industry standard common operational SAN Switch functionality	
	Warranty	5 Years full warranty (all parts replacement and 24x7 service) from Manufacturer and bidder should submit the OEM provided part number against the support requirement.	

4.RACK, KVM, Basic PDU and ATS

Sl. #	Item Descriptions	Required Specification	Bidder response
01	Brand	APC/HPE/Emersion/Oracle	
1.1	Model	To be mentioned by the bidder	
1.2	Country of Origin	USA/EU/JAPAN/UK	
1.3	Country of Manufacturer	To be mentioned by the bidder	
1.4	Dimension	Minimum 42U Height, 600 MM Width X 1070 MM Depth	
1.5	Rack Height	42 U	
1.6	Rack Width	19"	
2.0	KVM Console and Other accessories	Brand: Same as Rack brand Minimum 01U 17" in or higher Standard Console with 8 Port Switch and necessary cables.	

3.0	PDU	Brand: Same as Rack brand Two (2) Basic PDU, Zero U, 10A,230V, (15)C13	
4.0	ATS	Automatic Transfer Switches	
4.1	Capacity	16Amp	
4.2	Input Connection	IEC-320 C20	
4.3	Output Connection	(1) IEC 320 C19 (Battery Backup), (8) IEC 320 C13 (Battery Backup)	
4.4	Input Voltage	Nominal : 230V	
4.5	Output Voltage	Nominal : 230V; Total Current Draw : 162Amp	
4.6	Frequency	50/60 Hz	
4.7	Power Cable Length	Cord Length : 2.44meters ; Number of Power Cords : 1	
4.8	Max Input Current	20A	
4.9	Features	<ul style="list-style-type: none"> • 10 kAIC Overcurrent Protection • Wide range of input and output connections • Quick Transfer Rate • Dual Input Power Sources • Network Management Capabilities 	
4.10	Warranty	05 (Five) years full warranty with parts and labor	

Lot-2: Firewall and End Point Security

1. Next Generation Firewall (NGFW) Qty: 02 for HA

Sr.No	Parameter	Required Minimum Specifications	Compliance (Yes/No)	Bidder's Response
1	Brand	Please Mention		
2	Model	Please Mention		
3	Country of Origin	USA		
4	Form factor	Rack Mountable		
5	Hardware requirement	Minimum Port: 6 x 10/100/1000 BASE-T + 4 x 10/100/1000 SFP or SFP+		
		Appliance should have minimum 4GB DRAM and 8GB Flash		
		Should be an ASIC's based or Octa core or higher processor based solution for faster processing. Appliance should have minimum 30GB built-in storage		
		Redundant PSU from day 1 and power supply should be standard watts to make it power effective.		
6	Appliance Performance	The appliance should be capable of minimum 6 Gbps performance throughput		
		Firewall performance (IMIX) minimum 1.3 Gbps		
		Application Security minimum throughput – 2 Gbps		
		IPS minimum throughput – 2.2 Gbps		
		Appliance should be capable of minimum 650 Mbps of Routing + NAT + QoS + ACL performance throughput		
		Should support full DPI throughput of 670 Mbps or higher including Gateway Antivirus		
		Should support at least 4,000 IPSec (Internet Protocol Security) Site-to-Site VPN tunnels and 2000 or more number of IPSec Client Remote access VPN		
		Should support automatic ISP failover as well as ISP load sharing and load balancing for outbound traffic		
		Connections per second Minimum 35 K		
		Maximum concurrent sessions 300 K		

7	Routing Technology (from Day 1)	<p>Appliance should support the following IETF standards based protocols from Day 1:</p> <ul style="list-style-type: none"> - OSPF V1/2 - BGP - Route Based VLAN - Static Route <p>Router should support sourced based & policy based routing</p>		
8	QoS Requirement	<p>Appliance should support the following standard QOS features</p> <ul style="list-style-type: none"> - Class-based queuing with prioritization, - Queuing based on VLAN - interface - bundles, or filters, - Marking, -policing, - Control plane QOS 		
9	Security (from Day 1)	<p>Appliance should support the following standard Security features</p> <ul style="list-style-type: none"> - Stateful IPSec failover - Tunneling features like Supporting IPSec Encryption (DES, 3DES and AES), Message Support 		
10	Multicast	<p>Appliance should support multicast routing features on the appliance from day one/ policy based routing has to ensure</p>		
11	High Availability	<p>Appliance should support the following standard HA features</p> <ul style="list-style-type: none"> - Single license for primary and secondary firewall. Policies will be same for all features. 		
12	Reporting and Logging	<ul style="list-style-type: none"> -Appliance should support the following standard Reporting features. -Appliance should support bandwidth provisioning and reporting for individual application based utilization. -Appliance should be capable of supporting SIEM platform <p>All features to be available day one.</p>		
13	IPV6 (from Day 1)	<ul style="list-style-type: none"> -Appliance should support the following standard IPV6 features. -Appliance should support IPV6 routing. -All features to be available day one. 		
14	Management	<ul style="list-style-type: none"> -Appliance should support the following standard Management features -Appliance should support Administrative AAA access (RADIUS/XAUTH+) with granular access control for admins i.e. read-only, full-access etc. -Appliance Should support LDAP and SSO 		

		Router should support Citrix -Appliance should Support CAC		
15	Unified Threat Management Features	Antivirus - Should use an integrated scanning engine and virus signature databases to protect against viruses, trojans, rootkits, worms, and other types of malicious code from reaching devices on the network and throughput should not be less than 2.2 Gbps		
		Web filtering - Should allow permitting or blocking access to specific websites individually or based on the categories to which the website belongs.		
		Content filtering - Should provide basic data loss prevention functionality and should filter traffic based, file extension, and protocol commands.		
		IPS - Should have protocol anomaly detection, attack pattern obfuscation, Stateful protocol signatures and throughput not less than 2.1Gbps		
16	Certifications	The equipment should have USGv6, NDPP (Firewall and IPS), FIPS-140-2 Level 2, CsFC from Day 1		
17	Authorization	Original Manufacturer Authorization Certificate to be submitted along with the bid		
18	Training	The vendor must provide adequate and appropriate training to at least 2 (Two) personnel for efficient operation of the Security system at OEM Regional Location with all expenses.		
19	Warranty	Should have 05 years OEM Warranty and bidder Should quote the manufacturer support part code.		

2. Email Security

SI #	Specifications	Compliance
1	The Solution should be Hardware appliance based	
2	The solution should provide unlimited domain support	
3	The solution should support split mode architecture with separate Email Scanner Appliance & Separate Software based	

	Manager.	
4	The Email Security solution should provide flexible & scalable deployment options.	
5	The solution should support high email flow supporting 200 Users for now and should be scalable.	
6	The same solution should be scalable to support 1000 users of Email Security Infrastructure in future without need for replacing the Appliance.	
7	The Email Security Solution should also be able to get the updates through a Proxy Server if required.	
8	The solution should provide redundancy for both scanner and control center.	
9	Should combine antimalware technology with advanced heuristics to provide real-time email protection against viruses, spyware, phishing, and other malicious attacks while enforcing content filtering policies on Microsoft Exchange Server 2013 above.	
10	Ability to scan messages in transit or on the mailbox to protect against email borne threats.	
11	Advanced content filtering protects sensitive information using pre-defined policies, regular expressions, attachment criteria, true file typing, and more. Microsoft Active Directory® based enforcement.	
12	Support for Zimbra/Microsoft Exchange Database Availability Group.	
13	Flexible real-time, scheduled, and manual scanning.	
14	In-memory scanning and effective multi-threading for superior performance.	
15	5 years comprehensive Onsite Warranty, Support & Subscription from the Manufacturer.	
16	Device should minimum have 8 GB RAM	
17	Device should minimum have 500 GB built in storage	
PROTECTION		
1	It should provide Phishing Detection Technology	
2	Should contain Superior Spam Blocking Techniques	
3	Provide Directory Harvesting Attack Protection for emails.	
4	It should protect against denial of service attacks.	
5	Anti-spoofing with support for SPF, DKIM and DMARC should be available.	
6	Policy Rules for Users, Groups or All Users	
7	Compliance Rules and Routing Support	
8	Should support Email Encryption	
9	Ability to scan email attachments	
10	Should provide reputation based protection against bad emails/domains.	
11	Zombie Detection & Time-Zero Virus Protection with multiple scan engine module.	
12	Solution should provide inbound/outbound protection for	

	emails.	
13	Provision of connection management with advanced IP reputation should be available.	
14	Anti-spoofing with support for SPF, DKIM and DMARC	
15	Zombie detection	
16	The feature of adjusting the Spam Aggressiveness should be available.	
17	Advance threat protection should provide 100% catch rate and should be validated by reputed sources like NSS labs or equivalent	
18	Different level of Spam aggressiveness should be readily available. Ex: Medium, Strong etc.	
19	Ability to perform heuristics for email traffic.	
20	Should support Bayesian scanning and sandbox module for zero day protection with multiscan engine support	
COMPLIANCE/ENCRYPTION		
1	Robust policy management,	
2	Attachment scanning	
3	Approval boxes/workflow	
5	Dictionaries	
6	Encryption of emails should be provided as an option.	
7	Searches for predefined social security numbers, bank routing numbers or credit card numbers. An easy-to-use, web-based UI enables custom record searches.	
8	Attachment scanning—Looks for content within document attachments, including Word, PowerPoint, PDF and more than 300 other file types to ensure that sensitive data is not distributed.	
9	Set and enforce policies for common compliance setups	
10	Enable organizations handling health or financial records to monitor for HIPAA, SOX or GLBA violations. When these dictionaries are used in conjunction with Record ID matching, they ensure the Protection of confidential information.	
11	Enable the viewing of email that potentially violates compliance policies before allowing it to be distributed outside the organization.	
12	Device should also support Multi engine Advanced Threat Protection and should be available from Day 1	
13	Archiving: organizations should be able to route email that matches a specific policy to an external archive.	
14	Securely routes email that matches a specific policy to an integrated, seamless cloud encryption server to ensure the secure exchange of Email containing sensitive customer data or confidential information.	
15	Should enables organizations to monitor and report on compliance-related email traffic.	
16	Email encryption service to ensure secure exchange of confidential information	
ADMINISTRATION		

1	Configuration of the solution should be easy to configure with initial setup wizard.	
2	The solution should provide secure management through Graphical User interface via https	
3	Detection of appliance through ICMP should by default be disabled.	
4	Auditing of emails should be readily available through the GUI	
5	The email security solution should have the possibility of Integrating with LDAP	
6	Have the ability for Per User Anti-Spam Aggressiveness should be available.	
7	Have the ability to provide Per User Allowed/Blocked Lists	
8	The MTA should provide high throughput for email processing.	
9	Record ID matching to easily search for predefined information	
10	Attachment scanning to stop the release of unauthorized information	
11	It should provide the options of Adding disclaimers for both inbound and outbound email.	
12	Should be able to block attachments by Size.	
13	Provide the option to limit the size of emails through the solution.	
REPORTING		
1	Scheduling of Reports for Emails should be available	
2	Compliance reporting should be part of the solution.	
3	Should provide a dashboard for monitoring emails Good Vs Bad Emails etc.	
Warranty and Subscription		
	Must ensure minimum 5 years OEM warranty and subscription.	

3. Endpoint Security Specification

Sl No.	Required Specifications	Compliance (Yes/No)
1	Must offer comprehensive client/server security by protecting enterprise networks from which includes virus protection, spyware, rootkits, bots, gray ware, adware, malware and other computer borne threats or mixed threat attacks or any emerging cyber attacks or zero day attack protection. The solution should be in the of Gartner's leader's quadrant for Endpoint for last 13 years.	
2	Solution must clean computers of file-based and network viruses plus virus and worm remnants (Trojans, registry entries, viral files)—through a fully-automated process.	
3	Must be able to reduce the risk of virus/malware entering the network by blocking files with real-time compressed executable files.	
4	Must include capabilities for detecting and removing rootkits	
5	Must provide Real-time spyware/gray ware scanning for file system to prevent or stop spyware execution	
6	Must have capabilities to restore spyware/gray ware if the spyware/gray ware is deemed safe	

7	Must have Assessment mode to allow first to evaluate whether spyware/gray ware is legitimate and then take action based on the evaluation	
8	Must clean computers of file-based and network viruses plus virus and worm remnants (Trojans, registry entries, viral files)—through a fully-automated process	
9	To address the threats and nuisances posed by Trojans, the solution should be able to do the following but not limited to :	
	9.1 Terminating all known virus processes and threads in memory	
	9.2 Repairing the registry	
	9.3 Deleting any drop files created by viruses	
	9.4 Removing any Microsoft Windows services created by viruses	
	9.5 Restoring all files damaged by viruses	
	9.6 Includes Cleanup for Spyware, Adware etc	
10	Must be capable of cleaning viruses/malware even without the availability of virus cleanup components. Using a detected file as basis, it should be able to determine if the detected file has a corresponding process/service in memory and a registry entry, and then remove them altogether	
11	Must provide Outbreak Prevention to limit/deny access to specific shared folders, block ports, and deny write access to specified files and folders on selected clients in case there is an outbreak	
12	Predictive Machine Learning	
a	Pre-execution machine learning (static analysis of file attributes)	
b	Post-execution machine learning (dynamic analysis of process behavior)	
c	Cloud-dependent analysis	
d	File Scan Vectors	
e	Web download	
f	Email attachment	
g	USB auto run	
h	Scan Actions	
i	Log Only	
j	Quarantine	
k	Terminate	
13	Early Ransom ware Protection	
a	Protection against unauthorized encryption or modification	
b	Block processes commonly associated with ransom ware	
c	Program inspection	
d	Automatically backup and restore file changed by ransom ware	
14	Web Reputation	
a	Web Reputation to prevent access to malicious websites with accurate and comprehensive rating algorithm.	
b	Provide protection against browser exploit	
c	Location Aware	
d	To have Web Reputation Logs for endpoint vulnerability analysis	
e	Able to send notification upon web reputation violations.	
f	To support Approved URLs list	
g	To manually add Approved URL into Approved URLs list	
h	Able to select available Web Reputation Security Level: High, Medium, or Low	
i	Able to submit Web Reputation Feedback	
j	Able to display Web Threat Notification for users	
k	Able to modify the content of Web Threat Notification for users	
15	Firewall	
a	Centrally managed firewall policies	
b	Centrally update firewall driver	
c	Able to detect & block Network viruses/worms without blocking	
d	Able to centrally update network virus patterns	
e	Able to define different firewall policies for online/offline client	
f	Shall support Intrusion Detection System with intrusion signature	
g	Able to support traffic based on: -	
h	(i) Direction (inbound / outbound)	
i	(ii) Protocol (TCP/UDP/ICMP)	
j	(iii) Destination ports	
k	(iv) Source and destination computers	
l	Supports tasteful inspection	

m	Supports Firewall Violation Outbreak Monitor	
n	Able to allow user to view Client Firewall Privileges	
o	Able to generate firewall logs when violation happens	
p	Able to display Firewall Violation Notification for client users	
12	Able to modify the content of the notification message	
13	Able to disable agent's Firewall on selected computers	
	12.2 Enable certification that a software is safe to reduce the likelihood of false positive detections or equivalent	
14	Must provide Real-time clock down of client configuration allow or prevent users from changing settings or unloading/uninstalling the software	
15	Users with the scheduled scan privileges can postpone, skip, and stop Scheduled Scan.	
16	CPU/memory(physical or virtual) usage performance control during scanning :	
17	15.1 Checks the CPU usage level configured on the Web console and the actual CPU consumption on the computer	
18	15.2 Adjusts the scanning speed if:	
19	15.2.1 The CPU usage level is Medium or Low	
20	15.2.2 Actual CPU consumption exceeds a certain threshold	
21	Should have a manual outbreak prevention feature that allows administrators to configure port blocking, block shared folder, and deny writes to files and folders manually	
22	Should have Integrated spyware protection and cleanup	
23	Should have the capability to assign a client the privilege to act as a update/master relay agent for rest of the agents in the network	
24	Shall be able to perform different scan Actions based on the virus type (Trojan/ Worm, Joke, Hoax, Virus, other)	
25	shall be able to scan only those file types which are potential virus carriers (based on true file type)	
26	Should be able to detect files packed using real-time compression algorithms as executable files.	
27	shall be able to scan Object Linking and Embedding (OLE) File	
28	Must provide Web threat protection by the following ways:	
29	Must provide File reputation service	
	29.1 Must be able to check the reputation of the files hosted in the internet	
	29.2 Must be able check the reputation of the files in webmail attachments	
	29.3 Must be able to check the reputation of files residing in the computer	
30	Must protect clients and servers on the network, high performance network virus scanning, and elimination.	
31	Must provide the flexibility to create firewall rules to filter connections by IP address, port number, or protocol, and then apply the rules to different groups of users	
32	Must have smart feedback to enable feedback from the client agents to the threat research centers of the vendor.	
33	Uses any alternate method other than the conventional pattern based scanning with the following features:	
	33.1 Provides fast, real-time security status lookup capabilities in the cloud	
	33.2 Reduces the overall time it takes to deliver protection against emerging threats	
	33.3 Reduces network bandwidth consumed during pattern updates. The bulk of pattern definition updates only need to be delivered to the cloud or some kind of repository and not to many endpoints	
	33.4 Lowers kernel memory consumption on endpoints. Consumption increases minimally over time.	
34	Should be able to deploy the Client software using the following mechanisms:	
	34.1 Client installation Package (Executable & Microsoft Installer (MSI) Package Format), should support silent installer, unmanaged clients, specific installer for servers	
	34.2 Web install page	
	34.3 Login Script Setup	
	34.4 Remote installation	
	34.5 From a client disk image	
35	Must provide a secure Web-based management console to give administrators transparent access to all clients on the network	

36	The management server should be able to download updates from different source if required.	
37	Must reduce network traffic generated when downloading the latest pattern by downloading only incremental patterns.	
38	Must have the flexibility to roll back the Virus Pattern and Virus Scan Engine if required via the web console	
39	Should have role based administration with active directory integration	
	39.1 To create custom role type	
	39.2 To add users to a predefined role or to a custom role	
40	Should have integration with the Active directory 2008/2012 or higher	
41	Shall support grouping of clients into domains for easier administration	
42	Establish separate configuration for internally versus externally located machines (Policy action based on location awareness)	
43	Must be capable of uninstalling and replacing existing client antivirus software and to ensure unavailability of any residual part of the software.	
44	Must support plug-in modules designed to add new security features without having to redeploy the entire solution, thereby reducing effort and time needed to deploy new security capabilities to clients and servers across the network.E.g. Mobile Security, etc.	
45	Security Compliance should leverage Microsoft Active Directory services to determine the security status of the computers in the network	
46	The solution should support client installation on all the following:	
	46.1 Windows XP/Server 2003 32-bit Edition & 64-bit Edition	
	46.2 Windows 7, Window 8, Windows 10 (32-bit version & 64-bit version) and higher version if any	
	46.3 Microsoft Cluster Server having all applicable versions	
	46.4 Microsoft Windows Server 2008/2012/2016/2019 with all its versions	
	46.5 Client/solution installation on operating systems hosted on virtualization environment.	
	46.6 Should support Intel x64 , AMD x64 , any other variants of processor	
	47.7 Must be able to send notifications whenever it detects a security risk on any client or during a security risk outbreak, via E-mail, SMS, SNMP trap	
47	Should have a feature similar to Firewall Outbreak Monitor which sends a customized alert message to specified recipients when log counts from client IPS, client firewall, and/or network virus logs exceed certain thresholds, Signaling a possible attack.	
48	Must be able to send a customized notification message to specified recipients when firewall violations exceed certain thresholds, which may signal an attack	
49	Should perform Boot & Rootkit scan and cleaning	
50	Virus definition files should be lighter so that same can be transmitted to remote locations having weaker link or the update pattern size should be less than 200Kb	
51	System should be configured in such a way that at no case no endpoints/remote agents will be able to communicate with OEM cloud for obtaining updates through internet.	
52	In case of bot infection, bot removal tools also to be facilitated to clean the infected machine	
53	The solution should have latest machine learning technology in built from day one.	
54	The End point AV should have the option of integration with on premises sandbox/anti-apt appliance.	
55	The solution should have the option of the endpoint vulnerability shielding in the network.	
56	The solution should have ransom ware protection in built.	

General note for all products

All necessary installation (Hardware and Software) materials are to be supplied with the device as required for full and smooth functioning of the device. One copy of warranty certificate is to be given to the users at the time of delivery of the Device .Warranty for the Device must be provided as full on-site Warranty covering free parts & software including labor Vendor & OEM should support the appliance with all necessary upgrade for at least from the date of installation If any defect occurs during the stipulated warranty period, Supplier shall send his competent representative to **MF-CIB, Microcredit Regulatory Authority** site.



Business Finance for the Poor in Bangladesh (BFP-B)
Financial Offer for Supply of Server, Storage, Firewalls etc

Lot-1: Server, SAN Storage, SAN Switch, Rack

Serial	Item Name and Brief Description	Qty (Nos)	Unit Price (BDT)	Total Price (BDT)
1	Server Chassis: 2U Rack Mountable Rail kit, Processor: 2XIntel Xeon-Silver 4214 (2.2 GHz/12-core/85W) (2 Nos Processor) Core per Processor: 12 Core	3 Nos.		
2	SAN Switch Rack Mountable, Full duplex switch should support 24 ports with 8/16 Gbps FC connectivity with 12 active ports	2 Nos.		
3	Rack Including KVM, Basic PDU and ATS Any Brand compatible to Server Height: 42U Width 19" PDU brand same as Rack Brand Capacity: 16 Amp.	1 No.		
4	SAN Storage Storage Controller: Storage system should a unified system supporting all block and file protocols scaling to at 12 controllers (6 HA Pairs)	1 No.		
	Total in BD Taka			
	Total In GBP			

Amount in words BDT.....

Terms:

- 1.
- 2.
- 3.

Date:

Authorized Signature

Seal:



Business Finance for the Poor in Bangladesh (BFP-B)

Financial Offer for Supply of Server, Storage, Firewalls etc

Lot-2: Firewall, Email and End Point Security

Serial	Item Name and Brief Description	Qty (Nos)	Unit Price (BDT)	Total Price (BDT)
1.	Next Generation Firewalls With HA Rack Mountable	2 Nos.		
2.	Email Security As per details specification	Lot		
3.	End Point Security Client Server Based Antivirus As mentioned in details specifications	For 50 Users		
	Total in BD Taka			
	Total In GBP			

Amount in words BDT.....
.....

Terms:

- 1.
- 2.
- 3.

Date:

Authorized Signature

Seal: