



First Security Islami Bank Limited

ICT Division

Head Office

Plot#12, 2nd & 3rd Floor, Main Road.

Block # A, P.S- Badda,

Bashundhara R/A, Dhaka-1229.

Web: www.fsiblb.com; email: ict@fsiblb.com

Ref: FSIBL/HO/ICT/374/2023

Date: 03.05.2023

REQUEST FOR PROPOSAL (RFP)

For Purchasing 4 (four) units MZ Next Generation Firewall for DC and DR.

Bidder Reg. No.

Section A: General Information

SN	Item	Description
1	Name of the Bank	First Security Islami Bank Limited
2	Procuring Entity Name	Information & Communication Technology Division
3	Invitation of tender for	Supply & implementation of 4 (four) units MZ Next Generation Firewall at DC and DR as per technical specifications detailed in "Section C" hereunder from the eligible and registered Partners as specified in "Section B" hereunder.
4	Invitation for Quotation Ref. & Date	FSIBL/HO/ICT/374/2023 Date: 03.05.2023
5	Procurement Method	Open Tendering Method
6	Source of Fund	First Security Islami Bank Limited
7	Registration of bidders & price of Tender Document:	The interested eligible bidders have to enroll their name by submitting a prayer along with a non-refundable registration/enrollment fee Tk. 10,000.00 (Taka Ten Thousand) only in the form of "Payment Order" in favor of " First Security Islami Bank Limited " during submission of tender. No Tender documents will be sold physically. The bidder has to copy or download this tender document from the website: www.fsibld.com/tender and place them on their own letterhead to submit their bid.
8	Tender Process Dates & Times	Tender
		Registration
		Submission
		Opening Time
	Pre-bid Schedule	
9	Place of opening and receiving tender documents	First Security Islami Bank Limited, Plot#12, 3 rd Floor, Main Road. Block # A, P.S-Badda, Bashundhara R/A, Dhaka-1229.
10	Composition of bid Price shall be inclusive of	The costs of complete purchasing 4 (four) units MZ Next Generation Firewall as instructed by the bank, testing, commissioning, delivering to directed site and admissible VAT, excise duty, subsidiary duty, import duty, ATV, AIT etc. all types of taxes and revenues of the government and other regulatory authorities along with time value of money up to settlement of bills taking clearances from the end user of the bank.
11	Awarding the successful bidder	The bank may negotiate with the successful bidder or all bidders regarding price reduction modification, if necessary, before issuing the acceptance letter. A notification of award (NOA) will be provided by Bank to the successful bidder. Within 07 days of receipt of the Letter of Acceptance, the successful bidder shall sign a copy of it and return to the bank. Work must be completed within the time specified in the Work Order/Contract.
12	Payment & Security	The bidder shall furnish as bid security of 2.50% of the total financial offer in the form of bank draft or bank guarantee in the form of pay order or bank guarantee from any scheduled bank in favor of First Security Islami Bank Limited. The bid security shall be submitted along with the tender inside the envelop marked as "Financial Offer- for 4 (four) units MZ Next Generation Firewall for FSIBL DC and DR " The bid security should be valid for 60 days after the date of bid opening. Any bid not accompanied by

SN	Item	Description
		<p>an acceptable bid security shall be rejected as non-responsive. The bid security of unsuccessful bidders will be returned within 7 days from the date awarding the successful bidder. The bid security of the successful bidder will be returned when the bidder has signed the NOA and furnished the required performance security. The bid security may be forfeited if (a) the bidder withdraws its bid during the period of bid validity specified in the bid form; (b) if a successful bidder fails to sign the contract and (c) if a successful bidder fails to furnish the performance security.</p> <p>Within 07 days of receipt of the notification of award from the Bank, the successful bidder shall furnish as performance security of 10% of total amount in the form of pay order or bank guarantee from any scheduled bank in favor of First Security Islami Bank Limited. The performance security should be valid for 180 (one hundred eighty) days.</p> <p>Bid shall remain valid for a period of 3 (Three) months after the date of opening of the proposals. In exceptional circumstances, prior to expiry of the original bid validity period, the Bank may request the bidder to extend the period of validity for a specified additional period. The request and the responses shall be made in writing. A bidder agreeing to the request will not be permitted to modify its bid.</p> <p>50% payment of total price may be provided as an advance payment upon request of the successful bidder. 50% payment may be made after implementation of firewall with licenses in its environment upon getting satisfactory certificate from ICT Division, FSIBL, Head Office expressing clearly that the end user has no objection.</p> <p>In case of a failure of the successful Bidder to deliver next generation firewall with license in the prescribed time, the bidder will be liable to pay 0.5% of the Contract price as liquidated damages for every week after the deadline and will be deducted from the bill amount. The maximum penalty will be 10% of total contract price.</p>
13	Submission of bidders Qualifications/Eligibility and course of bidder	The interested registered bidder shall copy the "bidders' qualification" form from the webpage and place them on their own letterhead write their qualifications and individual information in a separate sealed envelope with proper labeling mentioning- "Bidder's Qualifications /Eligibility for supplying & implementation of Next Generation Firewall " license, Name of the bidder & Registration No.
14	Submission of Technical & Financial Offer	<p>The interested registered bidder shall copy the Asked Technical Specifications and Financial Offer form from the webpage and place them on their own letterhead and write their price offer for Section "C" and "D" in the designated field(s) and submit the document in a separate sealed envelope with proper labeling mentioning- "Financial Offer- for 4 (four) units MZ Next Generation Firewall for FSIBL Data Center", Name of the bidder & Registration No.</p> <p>The bidder should submit all financial and technical documents separately hard copy and soft copy by USB-Pen-drive during submission.</p>
15	Name and address of the Office for receiving tender(s)	CITO & Head of ICT Division. First Security Islami Bank Limited, Plot#12, 3 rd Floor, Main Road. Block # A, P.S- Badda, Bashundhara R/A, Dhaka-1229.
16	Address of Official Inviting Tender	Do.
17	Contact Details	Mobile: 01741018603, email: infosec@fsibld.com
18	Special Instruction	<p>The Bank Authority reserves the right to -</p> <ol style="list-style-type: none"> 1. Explain or clarify the terms of this tender notice in its own way, 2. Bring necessary changes in the notice 3. Increase or decrease the tender quantity 4. Reject the lowest 5. Reject any or all bids 6. Select any bidder deems fit and proper by them 7. Bidder have to bid full of the Section "C" & "D" <p>The bank authority can perform all the above things without assigning any reason. The bidder/supplier shall have no right to challenge the decision of the Bank Authority in any court of law or to any arbitrator.</p>

[Signature]



REQUEST FOR PROPOSAL (RFP)

For Purchasing 4 (four) units MZ Next Generation Firewall for DC and DR.

Tender Ref: FSIBL/HO/ICT/374/2023

Date: 03.05.2023

Bidder Reg. No.

Section B: Bidder's Information and Qualifications/Eligibility

SN	Description	Qualification	Response	Remarks
01	Name of the Bidder	Required		Attach NID copy
02	Designation of the Bidder	Required		
03	Company Name	Required		
04	Company Type [Proprietorship, Partnership, Private Limited, Public Limited etc.]	Required		
05	Website address of the company	Required		
06	Bidder's Office Phone No.	Required		Attach bill copy
07	Bidder's email address	Required		Send "Test" mail to infosec@fsibld.com
08	Bidder's Mobile No.	Required		
09	Verified Business Address	Required		Attach proof
10	Name of Contact Person	Required		Attach NID copy
11	Designation of the contact Person	Required		
12	Official email address	Required		Send "Test" mail to infosec@fsibld.com
13	Valid Trade License No.	Required		Attach proof
14	Valid VAT Registration No.	Required		Attach proof
15	Valid ETIN	Required		Attach proof
16	Valid IRC No.	Required		Attach proof
17	Authorization of the Principal	Required		Attach proof
18	Bank solvency certificate	Required		Attach proof
19	Are you adequately solvent to sale on? Credit for a period of 6 months or more?	Yes/No.		
20	Experience: The bidder must have 5 (Five) years of experience for supplying similar hardware & license in at least 5 (five) different reputed commercial bank in Bangladesh.	Required Bank- WO- Date- Quantity-		Attach proof
21	Are you Banned by any bank authority or? Government agency?	Yes/No		

Statement of the bidder: All the above information provided here in above are true. We will supply the order from genuine, valid and lawful sources and will pay all admissible VAT, Tax & other duties as per rule of the Government of Bangladesh.



REQUEST FOR PROPOSAL (RFP)

For Purchasing 4 (four) units MZ Next Generation Firewall for DC and DR.

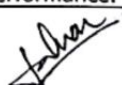
Tender Ref: FSIBL/HO/ICT/374/2023

Date: 03.05.2023

Bidder Reg. No

Section C: Technical/Financial Specifications of 4 (four) units MZ Next Generation Firewall for DC and DR.

Specifications: 4 (four) units MZ Next Generation Firewall for DC and DR.	
Description	Technical Specifications
Brand:	To be mentioned by the bidder
Model:	To be mentioned by the bidder
Country of Origin:	USA/EU
Environmental	Maintain International Quality Environmental Safety standard
Platform Requirement	The Next generation Firewall should be enterprise grade capacity for securing multisite network connectivity and provide user/server network protection against malware, exploits, and malicious websites in both encrypted and non-encrypted traffic. solution/hardware must be compatible with SDN and SD-WAN solution.
Form factor	Please mention RU with 19-inch rack mounting kits included
Part No	Bidder will mention details part number
3rd Party Certifications & Validation	ISO 9001/9002 for manufacturer for, FCC Class A/B for quality assurance The OEM must be recognized as a Leader in 2022 Gartner Magic Quadrant for Enterprise Firewalls.
Interface	The device should have minimum 8 X 1G Cu interfaces from day one 8 X 1G/10G SFP/SFP+ Interfaces from day one. The device should have scalability of minimum 4 x 40G QSFP+ or 4 x 25G SFP28 Interfaces/ports if required in future Bidder should quote 8 x 10G SFP+ module per unit The device should have dedicated 2 x 1G/10G HA Interface, 1 x Management, 1 x Console Interface.
Power Supply	The firewall must have dual hot-swappable AC power supplies
Memory	Minimum 32 GB DRAM from Day 1.
Architecture	The appliance hardware should be a multicore CPU architecture with a hardened 64 bit operating system to support higher memory or Proposed NGFW appliance (Each appliance) must have minimum 1 CPU with 12 Physical Cores from day 1
Virtual firewall/Virtual Domains/Context	The firewall should have minimum 6 Virtual firewall/Virtual Domains/Context Firewall should support configurable virtual systems resource limiting and management such as maximum/guaranteed 'active sessions' and log disk quota
High availability	Firewall should support Active-Active, Active-Passive & Clustering high availability from day one
Routing	Firewall should support Static, RIP, OSPF, IS-IS and BGP routing protocol.
NAT	Firewall should support static NAT, dynamic NAT, PAT, NAT64 and NAT46.
Firewall Performance (Day one)	A Minimum NG Firewall application throughput in real world/production environment (by enabling and measured with application control and logging enabled using 64 KB HTTP/appmix transactions – minimum 11 Gbps The firewall should support minimum 5.5 Gbps to above of Threat Protection (Firewall, IPS, Application Control, Malware Protection, Zero-day Protection and file blocking) throughput measured with enterprise mix traffic & logging enabled (utilizing 64 KB HTTP/appmix transactions) The bidder shall submit the performance test report from Global Product Engineering department / Global Testing Department/ Global POC team of OEM to certify the mentioned performance.



Signature & Seal of the bidder

	The firewall should support at least 10 Gbps of SSL Inspection (DPI) throughput or Max concurrent SSL decryption sessions of 140K
	The system shall accommodate at least 4,000 firewall policies
	Proposed appliance should support Minimum Concurrent Connection per second with threat prevention features enabled – 1.4 Million
	Proposed appliance should support Minimum New sessions per second –145K utilizing 1-byte HTTP transactions
	The firewall should support at least 6 Gbps IPSec VPN throughput
	The firewall should support at least 1,500 IPSec VPN tunnel
ATP (Advance Threat Protection) with Sandboxing/Wildfire/Zero-Day-Protection Features	The firewall shall allow organizations to implement both flow-based and proxy-based anti-malware concurrently, depending on the network and security needs
	Cloud based sandboxing of NGFW should support analysis of minimum 500000 files/Month
	The firewall shall provide ability to allow/monitor, block and quarantine attachments or downloads after malware detection
	The AV Engine should have AI malware detection model which integrated with regular AV scanning to help detect potentially malicious Windows Portable Executables (PEs) in order to mitigate zero-day attacks.
	The firewall shall support stream-based antivirus scanning for FTP, SFTP, and SCP protocols.
	The firewall shall support external block lists for domain names, web filtering URLs, IP addresses and malware hashes
	The firewall shall support real-time checksums DB of newly detected threats before AV signatures are available
	The antivirus scanning should be supported on various protocols not limited to HTTP/HTTPS, SMTP/SMTPS, POP3/POP3S, IMAP/IMAPS, MAPI, FTP/SFTP and CIFS
SSL Inspection Features	The firewall shall able to quarantine file and ban infected host
	The firewall should support DPI (Deep packet Inspection) for all types of traffic.
	The firewall shall provide Secure sockets layer (SSL) content scanning and inspection abilities that allow organizations to apply antivirus scanning, application control, web filtering, and email filtering to encrypted traffic
	The firewall shall support certificate inspection on port 443, all ports or a specific non-standard port.
	The firewall shall provide the ability to exempt web sites from SSL inspection by site reputation, address, category, or using a white list.
IPS	The system's IPS database shall have over 10,000 up-to-date signatures
	The firewall shall provide configurable IPS filters to selectively implement signatures based on severity, target (client/server), protocol, OS and Application types.
	The firewall shall support Allow session, Monitor and log session, Block session, reset session, quarantine attacker actions when an IPS attack is detected
	The IPS system shall able to scan botnet-connections to block Botnet C&C communication
Application Control	The firewall shall able to detect and take action against network traffic depending on the application generating the traffic.
	The firewall shall able to analyze network traffic to detect application traffic even if the traffic uses non-standard ports or protocols
	The firewall shall support detection for traffic using HTTP/2 protocol and able to block QUIC traffic so that browser automatically falls back to HTTP/2 + TLS 1.2
	The firewall shall support dynamic application filtering by querying real-time cloud-based categorization
	Application Control filtering engine should support Allow, block, reset session, monitor only and attacker quarantine actions when matched to a category
	The firewall shall support custom application signature
VPN Features	The firewall shall support industry standards of IPSEC, PPTP, L2TP and SSL without additional external solution, hardware or modules.
	The firewall shall support Route-based, policy-based IPSEC VPN and GRE over IPSEC
	The firewall shall support IKEv1 and IKEv2 to IPSEC VPN

Signature



Signature & Seal of the bidder

	The firewall shall support Local, Radius, LDAP and 2FA authentication for the VPN user
	The firewall shall support IPSec VPN encryption: DES, 3DES, AES128, AES192, AES256
	The firewall shall support IPSec VPN authentication: MD5, SHA1, SHA256, SHA384, SHA512
Authentication	The firewall should support LOCAL authentication user database
	The firewall should support RADIUS, TACACS, and LDAP remote authentication server
	The firewall should support Security Assertion Markup Language (SAML) authentication
	The firewall should support multi factor authentication (MFA)
	The firewall should support single-sign-on authentication
Cloud and SDN Integration	The firewall should have comprehensive SDN integration capabilities for AWS, Microsoft Azure, GCP, OCI, AliCloud, VMware ESXi, NSX, OpenStack, Cisco ACI and Nuage Virtualized Service Platforms
Log and Report	Must have built-in log and reporting module or vendor may offer additional appliance (HW/VM based) for log and reporting solution.
	Must be capable of providing rich reports based on application, users and threats or in any combination.
	Must support report generation on a manual or schedule (Daily, Weekly, Monthly, etc.) basis
	Must allow the report to be exported in PDF format
	Should support integration with SIEM tools like: Q-Radar, Arcsight, Splunk, Wazu etc.
Management Feature	The firewall should support complete GUI and CLI, HTTPS, SSH, Console, SNMP, API, Central Management.
	The firewall should have in-built CLI option in Graphical Interface for easy access in troubleshooting & configuration
	The firewall should have diagnostic CLI commands, session tracer, and packet capture for troubleshooting hardware, system, and network issues.
	The firewall should be able to manage network devices compliance via dynamic access control with tags provided by external security systems
	The firewall should have integration & automation technology with other security product to provide broader visibility, integrated end-to-end detection, threat intelligence sharing, and automated remediation
	The firewall should support Security Fabric Rating for the audit components within the fabric against best practices, provide results and recommendations, then allow users to easily apply remediations for some items
	The management platform must be capable of role-based administration, enabling different sets of views and configuration capabilities for different administrators subsequent to their authentication.
Security Features/Subscriptions	Must have at least following active security feature/subscription with the box from day one: <ul style="list-style-type: none"> - NGFW - Advanced Malware Protection - Anti Virus - Anti Spyware - SSL/TLS Traffic Inspection - APT and Sandboxing/Zero-Day Threat Protection - Application Control - Advanced IPS / NGIPS - Anti Botnet - VPN Gateway (IPSec & SSL)
Manufacturer's part number, Warranty/RMA and TAC support	Bidder must be submitted Manufacturer Authorization form (MAF)
	Bidder should submit BOQ of device including the details part numbers, 24x7 Premium (Elite) TAC support and manufacturer warranty for 3 year
	Bidder should quote necessary security subscription & license for 3 years
	OEM must have local depo to ensure faster RMA support within 3 working days.
All Accessories and Installation Materials	Original power cord, power cable, Mount kits, other necessary accessories and installation materials will have to be supplied by the supplier with the Devices/Items/systems as required for the full and smooth functioning of each device/Item/system.
Installation, Testing and Commissioning	Bidder must carry out on site installation, testing and commissioning. In consultation with IT Department, bidder must configure appropriate security and administration related policies, must do integration with other related hardware/software required to make the Network Functional and shall provide respective documentation to IT Division.

John



Signature & Seal of the bidder

REQUEST FOR PROPOSAL (RFP)

For Purchasing 4 (four) units MZ Next Generation Firewall for DC and DR.

Tender Ref: FSIBL/HO/ICT/374/2023

Date: 03.05.2023

Bidder Reg. No

Section D: User Training

Requirements	
1.	In-person on premises Installation and Administration training. The vendor / supplier must provide adequate and appropriate training to at least 10 bank personnel for an efficient operation of the System by an OEM certified trainer.
2.	A detailed training plan with specifications for Training courses, schedules, site and requirements must defined.
3.	The trainer should have at least 5 (five) years of expertise and delivered training on the specific domain on which training is being delivered.
4.	Training documentation have to be provided.

** The above-mentioned price is inclusive of all costs, taxes & VATs as per rule of the government of Bangladesh.

Name of the Bidder :
Designation of the Bidder :
Company Name :
Business Address :
Mobile No. :




Signature & Seal of the bidder