Bid Evaluation Report

Supply and Installation of Web Application Firewall (WAF-2)

1	Name of Procuring Agency	Sindh Bank Ltd.
2	Tender Reference No.	SNDB/COK/ADMIN/TD/1194/2021
3	Tender Description	Supply and Installation of Web Application Firewall (WAF-2)
4	Method of Procurement	Single Stage One Envelop Bidding Procedure
5	Tender Published & SPPRA S. No.	SPPRA S No. T00531-20-0025
6	Total Bid Documents Sold	01
7	Total Bids Received	01
8	Technical Bid Opening Date	09/04/2021
9	Financial Bid Opening Date	09/04/2021
10	No of Bid Technically Qualified	1
11	Bid(s) Rejected	0

S. No.	Name of Company	Cost Offered by Bidder	Ranking in Terms of Cost	Comparison with Estimated Cost (Rs.4,950,000/-)	Reason for Acceptance/ Rejection	Remarks
0	1	2	3	4	5	6
1	M/s Innovative Integration (Pvt) Ltd	Rs.4,746,915/-	Qualified Bidder	Rs.203,085/- below with the estimated cost	**Accepted** Being the Qualified Bidder	Rule 48 have been complied

Note: M/s Innovative Integration (Pvt) Ltd is selected for Supply and Installation of Web Firewall (WAF-2) to Sindh Bank Ltd being the qualified bidder.

Members – Procurement Committee **Signature**

(Mr. Saeed Jamal) Chief Financial Officer – EVP – Chairperson

(Col. Shahzad Begg) Head of Administration - EVP – Member

(Mr. Syed Muhammad Aqeel) Chief Manager, IDBL, KHI –AVP – Member

SINDH BANK
سندھ بینک

Date: 28-05-2021

Subject: **Certificate**
Compliance of SPPRA Rule 48
TENDER REF NO. SNDB/ADMIN/TD/1194/2021

This is to certify that as only one bid was received against the tender, so Rule 48 has been complied with detail as follows.

Market Price	Current Tender Price
Rs.6,094,605/- (Quotation Attached)	Rs.4,746,915/- (BER Attached)

S. Khurram Waheed
OG-I/I.T. Division

M. Rashid Memon
VP-I/I.T. Division

Members – Procurement Committee **Signature**

(Mr. Saeed Jamal) Chief Financial Officer – EVP – Chairperson

(Col. Shahzad Begg) Head of Administration – EVP – Member

(Mr. Syed Muhammad Aqeel) Chief Manager, IDBL, KHI –AVP – Member

Financial Proposal

Dated: Apr 20,2021

To,
Mr. Zeeshan,
Sindh Bank Karachi,

Subject: **Financial Proposal for F5 i2600 Awaf**

Submitted By:
Zain Ali
Key Account Manager,
FUTURE POINT TECHNOLOGIES
E-mail: zain.ali@futurepointt.com
Correspondence Address:
126, Sher Shah Block-New Garden Town Lahore.

FUTURE POINT TECHNOLOGIES

Attn:
Mr. Zeeshan,
Sindh Bank, Karachi

Date: Apr 20,2021
Ver: V-1
Ref No. FPT-20042021-

Dear Sir,

We are pleased to share our proposal for Revised Financial Proposal for F5 I2600 Awaf etc. We feel honoured to inform that Future Point Technologies is partner with some of the leading IT/Telecom solution providers such as Citrix, Cisco, VMWARE, EMC, Cisco, Juniper, Huawei, McAfee, Palo Alto, Fortinet, BDCOM, 3M etc. We are confident to deliver any size of project on turnkey basis.

Proposal for F5 I2600 Awaf								
S. No.	**Part. No.**		**Qty**	**Unit Price w/o Tax**	**Total Price w/o Tax**	**GST**	**Unit Price with Tax**	**Total Price with Tax**
1	F5-UPG-AC-I2XXX	BIG-IP Single AC Power Supply for i2X00 (250 W, Field Upgrade)	1	2,509	2,509	426	2,935	2,935
2	F5-BIG-AWF-I2600	BIG-IP i2600 Advanced Web Application Firewall (16 GB Memory, Base SSL, Base Compression)	1	24,185	24,185	4,111	28,297	28,297
3	F5-SVC-BIG-PRE-L1-3	BIG-IP Service: Premium (Service Length 12 Months)	1	3,798	3,798	646	4,444	4,444
4	F5-UPG-SFPO-R	BIG-IP & VIPRION SFP 1000BASE-T Transceiver (Field Upgrade)	2	539	1,079	92	631	1,262
				Grand Total USD	**31,570**			**36,937**

x 165 = 6,094,605

F5 i4600 AWAF only								
S. No.	**Part. No.**		**Qty**	**Unit Price w/o Tax**	**Total Price w/o Tax**	**GST**	**Unit Price with Tax**	**Total Price with Tax**
1	F5-UPG-AC-I4XXX	BIG-IP Single AC Power Supply for i4X00 (250 W, Field Upgrade)	2	2,509	5,017	17%	2,935.11	5,870.22
2	F5-BIG-AWF-I4600	BIG-IP i4600 Advanced Web Application Firewall (32 GB Memory, Base SSL, Base Compression)	2	42,569	85,139	17%	49,806.04	99,612.09
3	F5-SVC-BIG-PRE-L1-3	BIG-IP Service: Premium (Service Length 12 Months)	2	6,685	13,370	13%	7,821.59	15,643.17
	F5-UPG-SFP-R	BIG-IP & VIPRION SFP 1000BASE-SX Transceiver (Short Range, 550 m, Field Upgrade)	4	358	1,433	17%	419.30	1,677.18
				Grand Total USD	**104,960**			**122,802.66**

FPT Commercial Terms & Conditions:

Validity: Proposal will be valid for 15 days.

Above mentioned prices are subject to the quoted Quantity and prices may change with change in quantity.

2. There can be a subsequent clarification to this specific tender for which it is advised to keep yourself abreast with the notification being hoisted on Sindh Bank Ltd & SPPRA websites regularly.
3. Attachment of relevant evidence in eligibility criteria is mandatory. In case of non-provision of evidence in any of the requisite, bidder will be disqualified.
4. Bank reserves the right to verify all or any documents from the source, submitted in the bid as per SPPRA rule # 30(1).
5. Bank reserves the right to verify the equipment from the principle at any time to ensure that the supply of equipment is genuine, original, new and that its specification are the same as described in the bid.
6. In case of any fake/refurbished equipment, the company may be subject to legal proceeding as per SPPRA rule # 30(1).
7. Company will be considered disqualified if specification of the WAF quoted does not meet the specification given in the tender document.
8. Company shall supply Goods as per specifications and upon the recommendations of the Technical/Standardized Committee appointed by the Bank within 8 to 10 weeks from the date of receipt of purchase order. In addition to that Rs. 500/- per day will be fined after 10 days and Rs. 1,000/- per day will be fined after 20 days.

MANDATORY

1. GST/Income Tax Registration/Registration With Sindh Revenue Board
2. Attachment of Affidavit (specimen attached as Annexure "H") on stamp paper from the owner of the company.
3. Attachment of Annexure "A" (With Financial Proposal) & Annexure "B" (With Financial Proposal if Bank Guarantee is going to be submitted as Bid Security).
4. Writing of tender reference as given in the NIT on the Envelop, carrying tender document is must or the bank will not be responsible if the documents are not received by the Procurement Committee at the time of opening of bids.
5. The bidders are required to submit bids only in prescribed financial proforma given in Tender Document.
6. The representative present at the time of opening of tender shall be in possession of authority letter on the company's letter head, duly signed by the CEO of the company.
7. The Company must be in I.T. Business for Preferably 05 Years in Pakistan. (Attach documentary proof as Annexure-7)
8. Company must provide a valid & latest Manufacturer Authorization Certificate (MAF) from the Manufacturer/Principal for supply of required equipment.
   (Attach documentary/certificate proof as Annexure-8)

Note: Attachment of relevant evidence is mandatory in eligibility criteria. In case of non-provision of evidence in any of the requisite, bidder will be disqualified.

Taimoor Ghausi
AVP/ Finance Division.

Ahsan Ali
VP/ Operations Div

S. Zeeshan-ul-Haq
SVP/ I.T. Division

M/s Innovative Integration (Pvt) Ltd

Eligibility Criteria-WAF2

The prospective Supplier will provide Sindh Bank with two (02) Web application firewall (WAF) that includes the following features.

Bidder/OEM Eligibility Criteria:

The contract will be awarded to the successful Bidder whose bid will be found technically compliant and has offered the lowest cost and emerged as most advantageous bid. Proposed Bidder must qualify following criteria:

1. Bidder must be registered with Income Tax and Sales Tax Department and must appear on Active Taxpayer List of FBR.(YES/NO)
2. Bidder must either be a Manufacturer (OEM) or an authorized Partner of the OEM in Pakistan. (YES/NO)
3. Bidder must have Annual Turnover of at least PKR 15 Million in last Three (03) financial years. Audited Financial reports or Tax Statements to be submitted with the proposal. (YES/NO)
4. Bidder/OEM proposed solution must be deployed in at least Three (03) commercial Banks during last three years other than Sindh Bank. (YES/NO)
5. Bidder must have successfully done Two (02) deployments of Web Application Firewall (WAF) in commercial Banks last three years. (YES/NO)
6. Bidder must have service and support office in at least two (02) major cities of Pakistan including Karachi. (YES/NO)
7. Bidder must not be blacklisted by any government, semi-government, or private organization. (YES/NO)
8. Bidder must submit OEM authorization letter for this specific procurement. (YES/NO)
9. Quoted hardware / Software solution must have end of life beyond five (05) year at the time of submission. (YES/NO)
10. Bidder must be in relevant IT business since last Five (05) years. (YES/NO)
11. Bidder must have at least two professional level certified resource on proposed OEM. (YES/NO)
12. The proposed product must be recognized as a "Leader/Challenger" at-least once in last three (03) years of Gartner Magic Quadrant. (YES/NO)
13. Required quantities of Web application firewall (WAF) is Two (02) and will be deployed in Primary data center in High Availability (HA).

Qualified

ELIGIBILTY CRITERIA NOTE

1. If company not active Tax payer it will consider as a disqualified (Attached Proof as Annexcure-6).

Talmoor Ghausi
AVP/ Finance Division.

Ahsan Ali
VP/ Operations Div

S. Zeeshan-ul-Haq
SVP/ I.T. Division

DISQUALIFICATION

The bidder will be considered disqualified prior to/during technical/financial evaluation process or after award contract if:

1. On black list of SPPRA & Sindh Bank Ltd.
2. Issued with two (2) warning letters/emails by the Sindh Bank Ltd in the past to the bidder for unsatisfactory performances.
3. Not GST/Income Tax Registered/Registration With Sindh Revenue Board
4. Alternate bid is offered.
5. Non - Attachment of Annexure "A" (With Financial Proposal) & Annexure "B" (With Financial Proposal if Bank Guarantee is going to be submitted as Bid Security).
6. The qualified bidder sublets the contract in any form/stage to any other agency.
7. The tender is deposited without Tender Fee.
8. Warranty of supplied items is less than 1 year.
9. If during verification process of the cliental list the response by any of the bank is unsatisfactory on account of previous performance.
10. After supply, if the specification of supplied items is found different with the items produced in front of committee at the time of technical evaluation.
11. In the past, the company agreement has been prematurely been terminated after due qualification in any of the category of the tender.

Taimoor Ghausi	Ahsan Ali	S. Zeeshan-ul-Haq
AVP/ Finance Division.	VP/ Operations Div	SVP/ I.T. Division

M/S Innovative Integration (Pvt) Ltd

TENDER REF.NO. SNDB/COK/ADMIN/TD/1194/2021
(WAF-2)

SCOPE OF WORK / TECHNICAL SPECIFICATION

Sindh Bank requires Supply and Installation of Data Centre Web application firewall (WAF). The requirement will be issued on need basis. Therefore quantity may vary depends on the requirement of the bank, accordingly bank will not be responsible if the quantity asked is not as per scope of work below and in this context no claim will be entertained. Payment will be done on supply and installation of actual numbers of items.

The prospective Supplier will provide Sindh Bank with One (01) Enterprise-Class Next Generation Web application firewall (WAF) that include the following features.

Web application firewall (WAF) REQUIREMENTS:

SPECIFICATIONS

SN#	SPECIFICATIONS	
1	Intelligent Traffic Processing:	L7 requests per second: 350K L4 connections per second: 125K L4 HTTP requests per second: 600K Maximum L4 concurrent connections: 14M Throughput: 10 Gbps L4/L7
2	Hardware Offload SSL/TLS:	ECDSA: 2.1K TPS (ECDSA P-256) RSA: 2.5K TPS (2K keys) 5 Gbps bulk encryption*
3	Software Compression:	3 Gbps
4	Software Architecture:	64-bit TMOS
5	On-Demand Upgradable:	YES
6	Processor:	One 2-Core Intel Pentium processor (total 4 hyperthreaded logical processor cores)
7	Memory:	16 GB DDR4
8	Hard Drive:	1 TB Enterprise Class HDD
9	Gigabit Ethernet CU Ports:	Optional SFP
10	Gigabit Fiber Ports (SFP):	4 SX or LX (sold separately)
11	10 Gigabit Fiber Ports (SFP+):	2 SR/LR (sold separately); optional 10G copper direct attach

Policy Management

1. The WAF shall be able to automatically-built policies
2. The WAF shall be able to manually accept false positives by simple means (check box)
3. The WAF shall be able to define different policies for different applications
4. The WAF shall be able to create custom attack signatures or events
5. The WAF shall be able to customize Denial of Service policies
6. The WAF shall be able to combine detection and prevention techniques
7. The WAF shall have policy roll-back mechanism
8. The WAF shall be able to do versioning of polices
9. The WAF shall have a built-in real-time policy builder with automatic self-learning and creation of security polices
10. The WAF shall have application- ready security templates for applications - eg Microsoft Sharepoint, OWA, ActiveSync, SAP, Oracle Applications/Portal, PeopleSoft, Lotus Domino for
11. The WAF shall be capable of being restored to factory defaults
12. The WAF shall have the ability to automatically detect server technologies and suggest adding the detected server technologies to the user's security policy.
13. The WAF shall provide layered policies configuration in a hierarchical manner with a parent and child policies. This allows for quicker policy creation and learning. A security policy can be created in two ways:

Mohsin Ali Rahu AVP-II/ Admin. Div.	Kamal Rashid Officer Operation Div.	Atif Alvi AVP-II/I.T. Division

- Security Policy: This is similar to previous releases of an ASM security policy which can be applied to any relevant virtual server.
- Parent Policy: This is a new type of policy which enables the user to create a higher level policy to act as a template for its attached child policies.

14. The WAF layered policies configuration enhancements shall have the followings:
    - Administrators can mandate that all new security policies created must be attached to a compatible parent policy.
    - All attached child policies for a parent policy are listed in the parent policy details.
    - Parent policy suggestions now have a maximum score of parallel suggestions in its child policies. All locked child suggestions propagate to the parent policy. The score of the parallel suggestion in each child is shown in the parent policy pane per suggestion, with the top scoring children marked.
15. The WAF shall have an improved Policy Builder Process which has a single tabbed screen containing the configuration for a policy's General Settings, Inheritance Settings, Microservices, Attack Signatures, Threat Campaigns, and Response and Blocking Pages. The Policies List displays the name, enforcement mode, attached virtual servers and OWASP compliance.

Profile Learning Process

1. The WAF shall be able to recognize trusted hosts
2. The WAF shall be able to learn about the application without human intervention
3. The WAF shall be able to inspect policy (auditing + reporting)
4. The WAF shall be able to protect new content pages and objects without policy modifications
5. Able to provide anomaly learning of client integrity whether it is browser compared to automated web attack tool
6. Able to configure whether the system tracks sessions based on user names, IP addresses, or session identification numbers.
7. Positive security model support - An "allow what's known" policy, blocking all unknown traffic -and data types
8. Positive security model configuration
9. Application flow
10. Dynamic Positive security model configuration maintenance
11. Built in process engine to detect evasion techniques like cross site scripting Is there an out of the box rule database available.
12. Automated regular signature updates
13. Operates in a full Proxy architecture and inline control over all traffic through the WAF
14. Ability to hide back-end application server OS fingerprinting data and application specific information
15. Ability to protect against malicious activity within and hijacking of embedded client side code (javascript, vbscript, etc...)

Dynamic Web based defenses

1. The WAF shall be able to perform cloaking e.g hiding of error pages and application error pages and even specific data
2. The WAF shall be able to perform virus checking on HTTP file uploads and SOAP attachments. Support to Anti-Virus via ICAP communication channel
3. Provide protection of AJAX-enabled applications including those that use JSON for data transfer between the client and the server. This include support in set up AJAX blocking response behavior for applications that use AJAX, so that if a violation occurs on an AJAX request, the system displays a message or redirects the application user to another location.
4. The WAF shall support protection of XML Web Services
5. The WAF shall restricts XML Web Services access to methods defined via Web Services Description Language (WSDL) or XML Schema format (XSD)
6. The WAF shall be able to perform validation for Web Services XML Documents which is WS-I compliant
7. The WAF has a XML Parser Protection, limit recursions to thwart DoS conditions, limit the numbers of elements, lengths of elements, attack signatures enforcement. In addition, it can be used to encrypt and sign documents according to the WS-Security standard.
8. The WAF shall be able to perform information display masking/scrubbing on requests and responses
9. The WAF shall support Sensitive Data Masking for personal details about users and credit cards in the following entities:
    a. HTTP Header fields, especially Authorization
    b. URL segments with personal identification using positional parameters
    c. Cookie values
    d. HTTP Request body using positional parameters

Mohsin Ali Raho
AVP-II/ Admin. Div.

Kamal Rashid
Officer Operation Div.

Atif Alvi
AVP-II/I.T. Division

10. The WAF shall be able to monitor latency of Layer 7 (application layer) traffic to detect the spikes and anomalies in the typical traffic pattern to detect, report on, and prevent layer 7
11. The WAF shall be able to detect, report on, and prevent Layer 7 (application layer) brute force attack attempts to break in to secured areas of a web application by trying exhaustive, systematic permutations of code or username/password combinations to discover legitimate authentication credentials.
12. The WAF shall be able to detect, report on, and prevent Layer 7 (application layer) web bot doing recursive web scrapping and rapid surfing. It also has the abiilty to differentiate automated web attack agent from legit user. Provides the ability to customize the default list of recognized search engines, and add own site's search engine to the system's list of f. The WAF shall be able to integrate with these vulnerability testing tools - Whitehat sentinel, IBM Appscan, HP Webinspect and QualysGuard, for automated instant policy tuning. Provide unified IP address whitelists for Policy Builder trusted IP addresses, and anomaly whitelists (DoS Attack Prevention, Brute Force Attack Prevention, and Web Scraping Detection)
13. Provide GUI based control to determine the reputation of an IP address and operate (e.g. block) based on that reputation. The IP reputation database is regularly updated. It detect IP reputation based on:
    a. Windows Exploits: IP addresses that have exercised various exploits against Windows resources using browsers, programs, downloaded files, scripts, or operating system vulnerabilities.
    b. Web Attacks: IP addresses that have launched web attacks of various forms.
    c. Botnets: IP addresses representing compromised computers on the Internet that are now part of a botnet (machines that send spam messages, launch various attacks, or behave in other unpredictable ways).
    d. Scanners: IP addresses that have been observed to scan ports or networks, typically to identify vulnerabilities for subsequent exploits.
    e. Denial of Service: IP addresses that have launched denial of service attacks, often requests for legitimate services, but which occur at such a fast rate that targeted systems cannot respond and become overloaded or unable to service legitimate clients.
    f. Reputation: IP addresses that issue HTTP requests with a low average reputation, or that request only known malware sites.
    g. Phishing Proxy: IP addresses associated with phishing websites (sources that attempt to acquire information such as user names, passwords, and credit card details by masquerading as a trustworthy entity).

Detection techniques:

1. The WAF shall be able to support the following evasive detection techniques :
    a. URL-decoding
    b. Null byte string termination
    c. Self-referencing paths (i.e. use of /./ and encoded equivalents)
    d. Path back-references (i.e. use of /../ and encoded equivalents)
    e. Mixed case
    f. Excessive use of whitespace
    g. Comment removal (e.g. convert DELETE/**/FROM to DELETE FROM)
    h. Conversion of (Windows-supported) backslash characters into forward slash characters.
    i. Conversion of IIS-specific Unicode encoding (%uXXYY)
    j. Decode HTML entities (e.g. c, ", ª)
    k. Escaped characters (e.g. \t, \001, \xAA, \uAABB)
    l Negative security model techniques
    m. Implemented concepts to cover vulnerabilities (OWASP based):
2. The WAF shall be able to protect against:
    a. Unvalidated input
    b. Injection flaws
    c. SQL injection
    d. OS injection
    e. Parameter tampering
    f Cookie poisoning
    g. Hidden field manipulation
    h. Cross site scripting flaws
    i. Buffer overflows
    j Broken access control
    k. Broken authentication and session management
    l. Improper Error Handling
    m. XML bombs/DOS
    n. Forceful Browsing
    o. Sensitive information leakage

Mohsin Ali Raho	Kamal Rashid	Atif Alvi
AVP-II/ Admin. Div.	Officer Operation Div.	AVP-II/I.T. Division