# 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

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/-<br>(Quotation Attached) | Rs.4,746,915/-<br>(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

Atten:
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-SFPC-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<br>AVP/ Finance Division. | Ahsan Ali<br>VP/ Operations Div | S. Zeeshan-ul-Haq<br>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).

Taimoor 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<br>AVP/ Finance Division. | Ahsan Ali<br>VP/ Operations Div | S. Zeeshan-ul-Haq<br>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<br>L4 connections per second: 125K<br>L4 HTTP requests per second: 600K<br>Maximum L4 concurrent connections: 14M<br>Throughput: 10 Gbps L4/L7 |
| 2 | Hardware Offload SSL/TLS: | ECC†: 2.1K TPS (ECDSA P-256)<br>RSA: 2.5K TPS (2K keys)<br>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<br>(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 Raho
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 ability 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. &#99;, &quot;, &#xAA;)

    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
AVP-II/ Admin. Div.

Kamal Rashid
Officer Operation Div.

Atif Alvi
AVP-II/I.T. Division

p. Session hijacking
q. Denial of service
r. Request Smuggling
s. Cookie manipulation

3. The WAF shall be able to protect against New attack signatures
4. The WAF shall be able to protect against XML External Entities (XXE)
5. The WAF shall be able to protect against Insecure Deserialization
6. The WAF shall be able to protect against NoSQL Injection
7. The WAF shall be able to protect against Insecure File Upload
8. The WAF shall be able to protect against Server-Side Template Injection

**Application Delivery and Redundancy Capabilities:**

1. The WAF shall be able to support High Availability Failover via network only
2. The WAF shall be able to perform application level health check of the back end servers
3. The WAF shall be able to load balance to the back end servers (round robin, least connection, fastest response)
4. The WAF shall be able to support caching and compression in a single platform
5. The WAF shall be able to be implemented and installed on separate application delivery controller (ADC) hardware platforms
6. The WAF solution shall allow traffic pass through when the services fail. (Note that this is different from fail-open bypass)
7. The WAF shall be able to support vlan configuration through built in switch
8. The WAF shall be able to perform TCP/IP optimization
9. The WAF shall be able to perform packet filtering

**SSL capabilities:**

1. The WAF shall have SSL accelerators available for SSL offloading
2. The WAF shall store the certificate private key on the WAF using a secure mechanism
3. The WAF shall store the certificate private key on the WAF using a secure mechanism, and a passphrase
4. The WAF shall capable of communication to a backend application server using https
5. The WAF shall be capable of tuning the SSL parameters, such as SSL encryption method used, SSL version

**Other Mandatory Features:**

1. Able to support the prevention of sending or accessing cookies when unencrypted HTTP is the transport
2. Able to mitigates click-jacking attacks by instructing browsers not to load a page into a frame
3. Able to support generic scanner via a published XML schema
4. Mitigating Bots via Captcha (login wall).
5. Enable detection of anamolous traffic patterns that stem from a specific unique geo-location and allowing throttling of anomalous traffic by geo-location based on RPS counts.
6. Proactive BOT defense that provides always-on protection that prevent bot attacks driving Layer7 DOS attacks, webscrapping, and brute force attacks from ever taking place. Works with existing reactive anamoly detections. Introduces javascript challenge to slow requests down and distinguish bots before requests reach a server.
7. JS obfuscation and client side security. Adding an obfuscation mechanism to protect JS against examination or reverse engineering and tampering. The mechanism will run on the appliance as a Java background process compiling and obfuscating JS code - encrypting the code. This enhancement will ultimately hide sensitive information with JS, insert changeable data into JS files and allow a lock-free mechanism of syncing dynamically generated data including CAPTCHA and RSA key pairs.
8. The WAF shall support JSON protection.
9. The WAF shall support Single Page Application (SPA) protection by:

- Identifying the login page based on the Action Parameter.
- Detecting Nameless Parameters.
- Protecting Single Page Application Form submissions.
- Identifying the Username.
- Recognizing the JSON Content Profile better.

10. The WAF shall provide CSRF Protection with two enforcement modes:

- Verify CSRF Token
- Verify Origin

11. The WAF shall support simplified custom attack signature rule writing to allow users to create rules without needing to use Snort syntax or escape common characters.
12. The WAF shall support cookie modifications for the ASM policy and Device ID cookie names.
13. The WAF shall support Wildcards in Disallowed HTTP/HTTPS and WebSocket URLs

Mohsin Ali Raho
AVP-II/ Admin. Div.

Kamal Rashid
Officer Operation Div.

Atif Alvi
AVP-II/I.T. Division

14. The WAF shall support monitoring of resource utilization for request queue sizes with threshold alerts triggered and sent over local log, SNMP or SMTP. In this way, users can spot
15. The WAF shall allows the addition of a list of domains allowed to send out AJAX requests with custom headers for Single Page Applications. This prevents browsers from blocking cross domain AJAX requests while still enforcing a CORS (Cross Origin Requests) policy with single page applications.
16. The WAF shall support incidents exports in HTML format.
17. The WAF shall support Learning Suggestions exports in HTML format.
18. The WAF shall provide microservices security policy for a defined unique identifier of Hostname + URL.
19. The WAF shall provide Selective Security Live Software Updates which can receive scheduled and real time selective live updates of attack signatures, bot signatures, browser challenges,
20. The WAF shall have the OWASP Compliance Dashboard which details the coverage of each security policy for the top 10 most critical web application security risks as well as the changes
21 The WAF shall support HTTP/2 over SSL/TLS on both the client and server sides, without having to translate the client HTTP/2 traffic to HTTP/1.1 on the server-side.
22. The WAF shall log challenge failures in the event logs for Application Security and Bot Defense.
23. The WAF shall have PCI Compliance reporting which includes 2 options to automatically fix compliance issues to support PCI Compliance 3.2:
    - Encrypt transmission of cardholder data across open, public networks
    - User is forced to change password every 90 days.
24. The WAF shall have TLS fingerprints identification to distinguish between bad and good actors behind the same IP (NAT) and only block traffic from bad actors.
25. The WAF shall support Policy Change and Security Event Reporting to Continuous Integrations / Continuous Delivery (CI/CD) Servers for CI/CD Cycle Support. WAF deployment can be integrated within the user's CI/CD pipeline and user's DevOps tool chain for test and production environments. This allows the user to deploy the right WAF policy per each application

**Traffic Learning & Blocking:**

1. The WAF must able to configure a list of Allowed File Types for your web application
2. The WAF must be able to allow or disallow specific file type
3. The WAF must able to configure a list of Allowed URLs for your web application
4. The WAF must able to configure a list of Allowed Parameters for your web application
5. The WAF must able to configure a list of Allowed Cookies for your web application
6. The WAF must able to configure a list of Allowed HTTP Methods for your web application
7. The WAF must capable of blocking specific list of HTTP methods
8. The WAF must able to configure a list of Allowed Redirection Domains for your web application
9. The WAF must be able to enforce maximum length of following HTTP request parameters
    - URL Length
    - Query String (URL parameters) Length
    - Request Length
    - POST data size
10. The WAF must be able to enforce specific HTTP headers and values to be present in client requests
11. The WAF must support HTML5 Cross-Domain Request Enforcement to enable one website to access the resources of another website using JavaScript.
12. The WAF must be able to enforce specific HTTP headers and values to be present in client requests
13. The WAF must capable of defining parameters of own attack detection signatures and be alerted when thresholds for these are passed
14. The WAF must automatically download and apply new signatures to ensure up-to-date protection
15. The WAF must operate in a full Proxy architecture and inline control over all traffic
16. The WAF must be able to to hide back-end application server OS fingerprinting data and application specific information
17. The WAF must be able to protect against malicious activity within and hijacking of embedded client side code (javascript, vbscript, ect...)
18. The WAF must be able to mitigate DoS vectors focusing on protocol weaknesses of HTTP such as:
    - Slowloris
    - Slow Post
    - Hash DoS
    - HTTP Get Flood
19. The WAF must be able to detect DoS attacks by monitoring the average number of transactions per client IP addresses or individual requested URLs per second
20. The WAF must be able to detect DoS attacks by monitoring the average time it takes for the backend server to repspond to a specific URL. The WAF evaluates the response traffic from

21. the server to understand the Server Stress level to determine a DoS attack
22. The WAF must be able to detect, report on, and prevent Layer 7 (application layer) brute force attack attempts to

Mohsin Ali Raho
AVP-II/ Admin. Div.

Kamal Rashid
Officer Operation Div.

Atif Alvi
AVP-II/I.T. Division

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.

23. The WAF must be able to stop non-human attackers by presenting a character recognition challenge to suspicious users. This CAPTCHA challenge will be presented after the system detects one or more of the following issues:
- A suspicious IP address
- Requests from a suspicious country

24. The WAF must be able to mitigate traffic from countries that send suspicious traffic.
25. The WAF must be able to inject a JavaScript challenge instead of the original response in order to test whether the client is a legitimate browser or a bot.
26. The WAF must be able to protect Web Scraping from following criteria: Bot detection (Mouse and Keyboard activity and Rapid Surfing detection), Fingerprinting, Suspicious clients and
27. The WAF must support IP address whitelist and blacklist
28. The WAF must have capability of detecting non-browser based BOTs as part of the WAF advance BOTs detection capabilities
29. The WAF shall support the ability to disable individual attack signatures on HTTP headers, wildcard URLs and wildcard headers (*).
30. The WAF shall use proprietary correlation algorithms to aggregate reported events from non-staged traffic into user-understandable security issue incidents for quicker review and user
31. The WAF shall support "Potential Disallowed Files Type" List which may be seen in malicious requests, such as information leakage and remote code execution.
32. The WAF shall come with a preconfigured list which users can add to. T
33. he WAF shall automatically check all traffic for all policies against this list and can generate suggestions to amend a policy to add or remove
34. The WAF shall monitor and make suggestions for deletion on unobserved (inactive) entities similar to its suggestions for addition on observed entities in the Policy Building Process.
35. The WAF shall support client reputation mechanism which identifies bad sources, e.g. source IPs or device IDs, and contributes to an enhanced security policy enforcement and the prevention of false positive alerts. The Client Reputation score is used to prevent learning from malicious sources, e.g. vulnerability scanners, and improve the learning speed from The WAF shall support URL Positional Parameters as part of global parameters. The URL with positional parameters is a non-pure wildcard, e.g. /p/* or */cart/*/item/php.

**Behavioral DoS:**

1. The WAF shall support BADoS Unified Server Health Check Mechanism Based on L7 Analysis. The same virtual server predictive latency is now used for BADoS and Layer 7 DoS. This allows them to have the same trigger for stress and attack detection.
2. The WAF shall support BADoS DDoS Mitigation Based on Behavior Analysis and Integration with Whitelist. This provides administrators with the ability to exclude whitelist members from statistics collection, anomaly detection and mitigation. This feature also supports anomaly detection of X-Forwarded-For (XFF) HTTP headers.
3. The WAF shall provide BADoS automatic generation of Attack Request Signatures. Attackers are identified and marked as bad actors after their first appearance. This allows better policy enforcement when an attacker reappears thus sparing the remitigation process from BADoS.
4. The WAF shall support automatic threshold tuning in Layer 7 DoS TPS-based Detection and Stress-based Detection.
5. In TPS-based Detection, a single global threshold is calculated for each of the following entity types:
- Device ID
- Source IP
- URL
- Site Wide

6. In Stress-based Detection, the following thresholds are calculated:
- Device ID: Thresholds for up to the top 50 Device IDs are calculated and an additional threshold for all other Device IDs.
- Source IP: Thresholds for up to the top 100 source IPs are calculated and an additional threshold for all other source IPs. - URLs: Thresholds for up to the top 500 source URLs are calculated and an additional threshold for all other URLs.
- Site Wide: Single threshold

7. The WAF shall provide accelerated attack signature detection and mitigation for L4 DoS to handle very strong high rate DoS attacks.
8. The WAF shall be able to provide DoS-L7 Traffic Passive Monitoring via Switched Port Analyzer.

**Unified Bot Defense (Proactive Bot Defense & Anti-Bot Mobile SDK):**

1. The WAF shall support logging and reporting for Proactive Bot Defense which includes:
- A dedicated Bot Defense Request Log that displays each HTTP request along with its attributes.
- A Bot Defense Logging Profile to provide basic filtering capabilities in the Request Log and Remote Log. - Additional info and Blocking Page configuration in iRule.
- Transaction Outcome charts with filtering and drill-down capabilities.

Mohsin Ali Raho
AVP-II/ Admin. Div.

Kamal Rashid
Officer Operation Div.

Atif Alvi
AVP-II/I.T. Division

2. The WAF shall detect brute force attacks from sources identified by Username, Device ID or Source IP. The brute force functionality shall include:
    - Enforcement actions: CAPTCHA, Client Side Integrity, Honeypot and Drop.
    - Prevention for CAPTCHA bypass and Client Side Integrity bypass. - Distributed brute force attack protection.
    - Detection of Credentials Stuffing attacks using a dictionary of leaked or stolen credentials.
    - Prevention and Mitigation Duration are in minutes.
3. The WAF shall detect mobile application bots by identifying that the access is indeed a mobile app access and that the application is indeed untampered with. The WAF shall be able to extract a unique, non-Java Script, fingerprint for each mobile application instance and report client traffic composition per application for any given time period and what applications are used and the top URLs accessed. Mobile application detection is supported via a Software Development Kit (which requires minimal development and integration) and is supported
4. The WAF shall provide an Unified Anti-Bot Detection and Protection which covers bot signatures and proactive bot defense, and web scraping within a single Bot Defense profile.
5. The WAF shall have HTTP Header Sequence Behavioral Metric which can be used as a signature metric in distinguishing between real browsers and Bad Actor bots that have inaccurately
6. The WAF shall support CAPTCHA Sound to provide accessibility to the visually impaired. This default CAPTCHA response sound file can be replaced with a custom sound file.

**DataSafe (Application Level Encryption):**

1. The WAF shall support Single Page Applications (SPA) view for Application Level Encryption configuration on a login page.
2. The WAF shall allow parameter configuration in Application Level Encryption (DataSafe) based on all types of HTTP methods.
3. The WAF shall be able to create logging profiles to log information on client attempts to login to your protected website, and to log information on alerts sent by the BIG-IP system.
4. The WAF shall detect attempts to steal a user's password in the web browser when Password Exfiltration Detection is enabled on a protected URL. For this detection to be active, your URL must have a parameter set as Identify as Username and at least one parameter set as Substitute Value.

**API Security:**

1. The WAF shall provide Public APIs Protection by loading the Customer-specific OpenAPI files, which are in Swagger format, to the platform to automatically create a security policy
2. The WAF shall support JSON schema for user REST endpoints which can be uploaded to a JSON profile.
3. The WAF shall allow users to use Guided Configuration in ASM to configure API Security to protect API calls.
4. The WAF shall provide a API Protection Dashboard which displays API server health including security events that were flagged, such as web application attacks, bad source IP addresses, and malicious transactions. Users can use the dashboard for troubleshooting API Security.
5. The WAF shall support OpenAPI 3.0 Protection.

**Delivery Time**

Within 8 weeks

Mohsin Ali Raho
AVP-II/ Admin. Div.

Kamal Rashid
Officer Operation Div.

Atif Alvi
AVP-II/I.T. Division

## MINUTES OF THE OPENING OF THE TENDER (TECHNICAL /FINANCIAL PHASE)

TYPE OF PROCUREMENT ADMIN / IT / CONSULTANT / MEDIA

TENDER NAME Web Application Firewall (WAF)-2 (Need to Protect Web Application

TYPE OF TENDER SINGLE STAGE-ONE ENVELOPE / SINGLE STAGE-TWO ENVELOPE / TWO STAGE / TWO STAGE-TWO ENVELOPE

OPENING DATE 09-04-21

OPENING TIME 11:45 Am

ATTENDANCE (MEMBER PC)

| | NAME | FIRM |
|---|---|---|
| ATTENDANCE (REPS. OF BIDDERS) | | |
| | ① Innovative Integration (Pvt) Ltd | |

TOTAL BIDS ACCEPTED FOR EVALUATION

TOTAL BIDS REJECTED

REMARKS

SIGNATURE MEMBERS PC-ADMIN

Head - Fin Div.

Head - Admin Div.

Member- IDBL

Date:

Innovative Integration

SIGNATURE MEMBERS PC-ADMIN
Head - Fin Div. ____
Head - Admin Div. ____
Member IDBL. ____

Financial Proposal

**PRICE SCHEDULE**

(Applicable for the year 2021-2022)

Name of Bidder ______________________

| S.NO | Item | Unit Price | Quantity | Amount (PKR) |
|---|---|---|---|---|
| 1 | Web application firewall (WAF-2) | 4,746,915 | 1 | 4,746,915 |
|  | *Total Amount (In PKR) |  |  |  |

* This amount will be considered as only the "Bid Offered". Whereas be apprised that the successful bidder will be the one whose "Evaluated Bid" is the lowest. (For further clarification refer Note. 6 below).

Note

1. The total cost must include all applicable taxes, duties and other charges as mentioned in the description column, Stamp duty (as applicable under Stamp Act 1989), delivery charges upto Sindh Bank Limited branches on Countrywide basis
2. No advance payment for supply of goods will be made. bills are only be processed for necessary payment on receipt of certificate of delivery/satisfaction from the branch manager
3. Calculation of Bid Security 5% of the Grand Total Amount of the Financial Proposal will be submitted along with tender as Bid Security
4. In case it is revlled at any stage after supply of the goods/items that the asked specification of the tender have not been met, the amount of the supply of that specific goods will be fined to the vendor with appropriate action as deem necessary by the procurement committee
5. Qualified company will also be bound to sign a bond/undertaking that in case of any observation arising in respect of quality of the goods within the warranty period, the company will be liable to address it at his own cost, non-compliance of the same will result into initiation of a case against the company for non-commitment or cancellation of tender as will be decided by the Procurement Committee
6. Lowest evaluated bid is going to be the criteria for award of contract rather than considering the lowest offered bid, encompassing the lowest whole sum cost which the procuring agency has to pay for the duration of the contract. SPPRA Rule 49 may please be referred
7. All conditions in the contract agreement attached as Annexure G are part of this tender document
8. The tender will be considered cancelled if the contract agreement after due signature is not submitted with Admin Office after 5 days of completion of bid evaluation report hoisting period 3 days) on SPPRA website
9. In case financial bids are the same, the successful bidder will be the one who has acquired more marks in the technical evaluation
10. In case of over writing/cutting/use of Blanco is found in the Financial Bid document, the bid will be taken as null & void however if the figures are readable and are also duly signed only then, bid will be accepted
11. Contract agreement will be executed after deposit of 5% performance security of the total tender amount in shape of Pay Order/Bank Guarantee in favor of Sindh Bank Limited
12. Quality is ensured. In case it is revealed at any stage after supply of the items that the asked specifications of the tender have not been met, the performance security will be forfeited
13. Free backup facility in case the item is reported defective
14. Goods to be delivered have to be packed in such a way that no damage is reported by the branch on delivery. In case of any such complaint is received the bidder will replace that item at his own cost.
15. If the obligation of warranty period are not met or delayed, the repair etc. requirement on this account will be deducted from the performance security / upcoming payment due to supplier
16. *Payment will be made in Pak Rupee*

*Note. There can be subsequent modification or amendment to this specific tender for which it is advised to keep yourself abreast with the notification being hoisted on Sindh Bank Ltd. & SPPRA website regularly.*

*Signature & Stamp of Bidder* ______________________

SINDHBANK
POWER TO THE PEOPLE

ATTENDANCE SHEET
BID OPENING -

FOR SELECTION OF Web Application Firewall (WAF) - 2 (Help to Protect Web Application)

Date: 09-04-2021

| S.No | Company Name | Name of Company Representative | Contact No. | Company Address | Signature |
|---|---|---|---|---|---|
| 01 | Innovative Integration (Pvt.) | FARAZ Arif KHAN | 0332 3000526 | 2nd FLOOR ADEB BUILDING, 58 WEST WHARF ROAD | Faraz A Khan |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

Signature -Procurement Committee Members

Head of Administration

Chief Financial Officer

Chief Manager (IDBL)