

SINDH PUBLIC PROCUREMENT REGULATORY AUTHORITY

CONTRACT EVALUATION FORM

TO BE FILLED IN BY ALL PROCURING AGENCIES FOR PUBLIC CONTRACTS OF WORKS, SERVICES & GOODS

- 1) NAME OF THE ORGANIZATION / DEPTT. SINDH BANK LIMITED/ADMINISTRATION
- 2) PROVINCIAL / LOCAL GOVT./ OTHER SCHEDULED BANK
- 3) TITLE OF CONTRACT Supply & Installation of Web Application Firewall (WAF-I)
- 4) TENDER NUMBER SNDB/COK/ADMIN/TD/1193/2021
- 5) BRIEF DESCRIPTION OF CONTRACT Same as above
- 6) FORUM THAT APPROVED THE SCHEME Competent Authority
- 7) TENDER ESTIMATED VALUE Rs.14,850,000/-
- 8) ENGINEER'S ESTIMATE
(For civil works only) _____
- 9) ESTIMATED COMPLETION PERIOD (AS PER CONTRACT) 1 Year
- 10) TENDER OPENED ON (DATE & TIME) 09/04/2021 at 1130 Hrs
- 11) NUMBER OF TENDER DOCUMENTS SOLD 1
(Attach list of buyers)
- 12) NUMBER OF BIDS RECEIVED 1
- 13) NUMBER OF BIDDERS PRESENT AT THE TIME OF OPENING OF BIDS _____
- 14) BID EVALUATION REPORT 17/06/2021
(Enclose a copy)
- 15) NAME AND ADDRESS OF THE SUCCESSFUL BIDDER M/s. Innovative Integration (Pvt.) Ltd
2nd Floor, KOLB Bldg
West Wing 2F
- 16) CONTRACT AWARD PRICE Rs.14,260,106/-
- 17) RANKING OF SUCCESSFUL BIDDER IN EVALUATION REPORT
(i.e. 1st, 2nd, 3rd EVALUATION BID). 1. M/s. Innovative Integration (Pvt.) Ltd
- 18) METHOD OF PROCUREMENT USED : - (Tick one)
- a) SINGLE STAGE – ONE ENVELOPE PROCEDURE ☒ Domestic/ Local
- b) SINGLE STAGE – TWO ENVELOPE PROCEDURE ☐
- c) TWO STAGE BIDDING PROCEDURE ☐
- d) TWO STAGE – TWO ENVELOPE BIDDING PROCEDURE ☐

PLEASE SPECIFY IF ANY OTHER METHOD OF PROCUREMENT WAS ADOPTED i.e.
EMERGENCY, DIRECT CONTRACTING ETC. WITH BRIEF REASONS:

19) APPROVING AUTHORITY FOR AWARD OF CONTRACT _____

20) WHETHER THE PROCUREMENT WAS INCLUDED IN ANNUAL PROCUREMENT PLAN?

Yes	<input checked="" type="checkbox"/>	No	<input type="checkbox"/>
-----	-------------------------------------	----	--------------------------

21) ADVERTISEMENT :

i) SPPRA Website
(If yes, give date and SPPRA Identification No.)

Yes	SPPRA NIT ID:T00531-20-0025
No	

ii) News Papers
(If yes, give names of newspapers and dates)

Yes	Express Tribune, Daily Express & Sindhi Express (24/03/2021)
No	

22) NATURE OF CONTRACT

Domestic/ Local	<input checked="" type="checkbox"/>	Int.	<input type="checkbox"/>
--------------------	-------------------------------------	------	--------------------------

23) WHETHER QUALIFICATION CRITERIA
WAS INCLUDED IN BIDDING / TENDER DOCUMENTS?
(If yes, enclose a copy)

Yes	<input checked="" type="checkbox"/>	No	<input type="checkbox"/>
-----	-------------------------------------	----	--------------------------

24) WHETHER BID EVALUATION CRITERIA
WAS INCLUDED IN BIDDING / TENDER DOCUMENTS?
(If yes, enclose a copy)

Yes	<input checked="" type="checkbox"/>	No	<input type="checkbox"/>
-----	-------------------------------------	----	--------------------------

25) WHETHER APPROVAL OF COMPETENT AUTHORITY WAS OBTAINED FOR USING A
METHOD OTHER THAN OPEN COMPETITIVE BIDDING?

Yes	<input type="checkbox"/>	No	<input checked="" type="checkbox"/>
-----	--------------------------	----	-------------------------------------

26) WAS BID SECURITY OBTAINED FROM ALL THE BIDDERS?

Yes	<input checked="" type="checkbox"/>	No	<input type="checkbox"/>
-----	-------------------------------------	----	--------------------------

27) WHETHER THE SUCCESSFUL BID WAS LOWEST EVALUATED
BID / BEST EVALUATED BID (in case of Consultancies)

Yes	<input checked="" type="checkbox"/>	No	<input type="checkbox"/>
-----	-------------------------------------	----	--------------------------

28) WHETHER THE SUCCESSFUL BIDDER WAS TECHNICALLY
COMPLIANT?

Yes	<input checked="" type="checkbox"/>	No	<input type="checkbox"/>
-----	-------------------------------------	----	--------------------------

29) WHETHER NAMES OF THE BIDDERS AND THEIR QUOTED PRICES WERE READ OUT AT
THE TIME OF OPENING OF BIDS?

Yes	<input checked="" type="checkbox"/>	No	<input type="checkbox"/>
-----	-------------------------------------	----	--------------------------

30) WHETHER EVALUATION REPORT GIVEN TO BIDDERS BEFORE THE AWARD OF
CONTRACT?
(Attach copy of the bid evaluation report)

Yes	<input checked="" type="checkbox"/>	No	<input type="checkbox"/>
-----	-------------------------------------	----	--------------------------

31) ANY COMPLAINTS RECEIVED
(If yes, result thereof)

Yes	
No	No

32) ANY DEVIATION FROM SPECIFICATIONS GIVEN IN THE TENDER NOTICE / DOCUMENTS
(If yes, give details)

Yes	
No	No

33) WAS THE EXTENSION MADE IN RESPONSE TIME?
(If yes, give reasons)

Yes	
No	No

34) DEVIATION FROM QUALIFICATION CRITERIA
(If yes, give detailed reasons.)

Yes	
No	No

35) WAS IT ASSURED BY THE PROCURING AGENCY THAT THE SELECTED FIRM IS NOT
BLACK LISTED?

Yes	<input checked="" type="checkbox"/>	No	<input type="checkbox"/>
-----	-------------------------------------	----	--------------------------

36) WAS A VISIT MADE BY ANY OFFICER/OFFICIAL OF THE PROCURING AGENCY TO THE
SUPPLIER'S PREMISES IN CONNECTION WITH THE PROCUREMENT? IF SO, DETAILS TO
BE ASCERTAINED REGARDING FINANCING OF VISIT, IF ABROAD:
(If yes, enclose a copy)

Yes	<input type="checkbox"/>	No	<input checked="" type="checkbox"/>
-----	--------------------------	----	-------------------------------------

37) WERE PROPER SAFEGUARDS PROVIDED ON MOBILIZATION ADVANCE PAYMENT IN
THE CONTRACT (BANK GUARANTEE ETC.)?

Yes	<input type="checkbox"/>	No	<input checked="" type="checkbox"/>
-----	--------------------------	----	-------------------------------------

38) SPECIAL CONDITIONS, IF ANY
(If yes, give Brief Description)

Yes	
No	no

Signature & Official Stamp of
Authorized Officer

Lt Col (R) Shahzad Begg
EVP/Head of Administration
SINDH BANK LIMITED

2/7/21

FOR OFFICE USE ONLY

SPPRA, Block. No.8, Sindh Secretariat No.4-A, Court Road, Karachi
Tele: 021-9205356; 021-9205369 & Fax: 021-9206291

Print

Save

Reset

Bid Evaluation Report						
Supply and Installation of Web Application Firewall (WAF-1)						
1	Name of Procuring Agency	Sindh Bank Ltd.				
2	Tender Reference No.	SNDB/COK/ADMIN/TD/1193/2021				
3	Tender Description	Supply and Installation of Web Application Firewall (WAF-1)				
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	Bids Rejected	0				

S. No.	Name of Company	Cost Offered by Bidder	Ranking in Terms of Cost	Comparison with Estimated Cost (Rs.14,850,000/-)	Reason for Acceptance/ Rejection	Remarks
0	1	2	3	4	5	6
1	M/s Innovative Integration (Pvt) Ltd	Rs. 14,260,106/- @Rs. 7,130,053/- per unit for 2 Firewalls	Qualified Bidder	Rs. 589,894/- 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-1) to Sindh Bank Ltd being the qualified bidder.

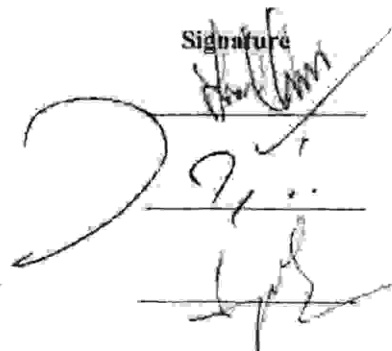
Members – Procurement Committee

(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

Signature





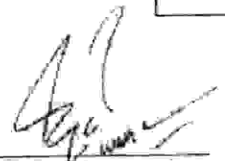
Date: 28-05-2021

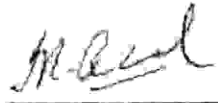
Subject:

Certificate
Compliance of SPPRA Rule 48
TENDER REF NO. SNDB/ADMIN/TD/1193/2021

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.20,262,330/- for 2 Unit (Quotation Attached)	Rs.14,260,106/-for 2 Unit (BER Attached)


S. Khuram Waheed
OG-I/T. Division


M. Rashid Memon
VP-I/T. Division

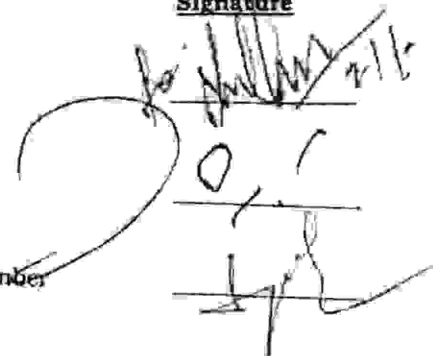
Members - Procurement Committee

(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

Signature



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 126, Sher Shah Block-New Garden Town Lahore.

FUTURE POINT TECHNOLOGIES

Attention:
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 Awaif 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 Awaif								
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	4.11 1	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-SFP-C-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
F5 i4600 AWAIF 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.

FUTURE POINT TECHNOLOGIES 126, Sher Shah Block-New Garden Town Lahore.

= 20,262,330/-

INFORMATION:

This Proposal has been prepared solely based on information supplied to FUTURE POINT TECHNOLOGIES by you. FUTURE POINT TECHNOLOGIES has relied on the correctness, accuracy and completeness of the information provided by you. FUTURE POINT TECHNOLOGIES takes no responsibility and has no liability for or in respect of the information provided by you. FUTURE POINT TECHNOLOGIES reserves the right to make changes to the Proposal and/or the pricing of this Proposal if, at any time after you accept this Proposal, any information provided by you proves to be incorrect, inaccurate or incomplete.

Excusable Events:

FUTURE POINT TECHNOLOGIES shall not be liable or considered in breach of its obligations under this Contract to the extent that FUTURE POINT TECHNOLOGIES's performance is delayed or prevented, directly or indirectly, by any cause beyond its reasonable control, or by armed conflict, acts or threats of terrorism, epidemics, strikes, lockouts, Changes of Statutory Regulations, Governments Measures of decree or other labour disturbances, or acts or omissions of any governmental authority or of the Buyer or Buyer's contractors or suppliers. If an excusable event occurs, the schedule for FUTURE POINT TECHNOLOGIES's performance shall be extended by the amount of time lost by reason of the event plus such additional time as may be needed to overcome the effect of the event. If acts or omissions of the Buyer or its contractors or suppliers cause the delay, FUTURE POINT TECHNOLOGIES shall also be entitled to an equitable price adjustment.

Payment terms:

For Hardware 70% advance & 30% within 30 days after hardware delivery.

For Services 50% advance & 50% after completion of Job.

No order cancellation allowed, once order processed by FUTURE POINT TECHNOLOGIES.

All Taxes will be charged as per governing laws of that region.

Purchase Order & Payment to be processed in favor of M/s 'FUTURE POINT TECHNOLOGIES'

Prices are subject to change in accordance with the any change in government policy, FED, levies, taxes & duties

All the sales will be subject to sales tax where applicable and customer will be withheld the tax at the time of payment if required by applicable law.

warranty:

Standard Manufacturer's Warranty (If applicable/ terms apply).

Force Majeure:

Prices are subject to change due to the change in currency (devaluation) or duty structure or taxation at any time of the transaction.

Note:

Prices are subject to change due to any change in duty/tax structure. The quote is based on current applicable Import duties/levies. If any change by competent authorities is made in the current Import duties, general sales tax, federal excise duty, special excise duty etc, the quote will be revised accordingly.

Best Regards:

Zain Ali

Key Account Manager,

FUTURE POINT TECHNOLOGIES

Mobile: 0300-0458117

E-mail: zain.ali@futurepoint.com

Correspondence Address:

126, Sher Shah Block-New Garden Town Lahore.

FUTURE POINT TECHNOLOGIES 126, Sher Shah Block-New Garden Town Lahore.

Eligibility Criteria-WAF1

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

Bidder/OEM Eligibility Criteria:

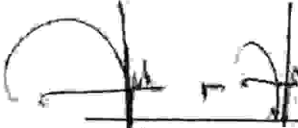
The contract will be awarded to the successful Bidder whose bid will be found technically compliant and has offered the lowest cost and emerged as most advantageous bid. Proposed Bidder must qualify following criteria:


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 50 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). ✓

ELIGIBILITY CRITERIA NOTE

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


Taimoor Ghausi
AVP/ Finance Division.


Ahsan Ali
VP/ Operations Div


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


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.

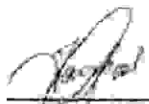

Ahsan Ali
VP/ Operations Div


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

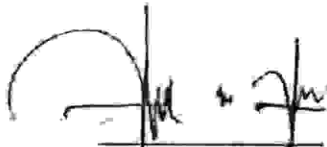
DISQUALIFICATION

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 client 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



Talmoor Ghausi
AVP/ Finance Division.



Ahsan Ali
VP/ Operations Div



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

Financial Proposal

SIGNATURE MEMBERS PC-ADMIN
 Head - Fin Div. _____
 Head - Admin Div. _____
 Member-TOR _____
PRICE SCHEDULE
 Date: _____
 (Applicable for the year 2021-2022)

Name of Bidder INNOVATIVE INTEGRATION PVT LTD

S.NO	Item	Unit Price	Quantity	Amount (PKR)
1	Web application Firewall (WAF-1)	7,130,053	2	14,260,106
*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

- 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.
- 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.
- Calculation of Bid Security 5% of the Grand Total Amount of the Financial Proposal will be submitted along with tender as Bid Security.
- In case it is revealed 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 deemed necessary by the procurement committee.
- 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.
- 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 agreement. SPPRA Rule 49 may please be referred.
- All conditions in the contract agreement attached as Annexure G are part of this tender document.
- 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 (holding period 3 days) on SPPRA website.
- In case financial bids are the same, the successful bidder will be the one who has acquired more marks in the technical evaluation.
- 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.
- 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.
- 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.
- Free backup facility in case the item is reported defective.
- 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.
- 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.
- 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 hosted on Sindh Bank Ltd. & SPPRA website regularly.

Signature & Stamp of Bidder

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 Two (02) 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: 650K L4 connections per second: 250K L4 HTTP requests per second: 1M Maximum L4 concurrent connections: 28M Throughput: 20 Gbps L4/L7
2	Hardware Offload SSL/TLS:	ECCT: 0.5K TPS (ECDSA/P-256) RSA: 10K TPS (2K keys) 10 Gbps bulk encryption*
3	Software Compression:	6 Gbps
4	Software Architecture	64-bit TMOS
5	On-Demand Upgradable:	YES
6	Processor:	One 4-Core Intel Xeon processor (total 8 hyperthreaded logical processor-cores)
7	Memory:	32 GB DDR4
8	Hard Drive:	1 TB Enterprise Class HDD
9	Gigabit Ethernet CU Ports:	Optional SFP
10	Gigabit Fiber Ports (SFP):	8 SX or LX (sold separately)
11	10 Gigabit Fiber Ports (SFP+):	4 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 policies
9. The WAF shall have a built-in real-time policy builder with automatic self-learning and creation of security policies
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.

Mohsin Ali Bano
AVP-II/ Admin, Div.

Kamal Rashid
Officer Operation Div.

Atif Alvi
AVP-II/I.T. Division

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:
 - 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
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

Mohsin Ali Raho
AVP-II/ Admin. Div.

Kamal Rashid
Officer Operation Div.

Atif Ali
AVP-II/I.T. Division

- 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 Webspect 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 Scrapping 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 (%uXXXX)
- 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
- 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

Mohsin Ali Raho
AVP-II/ Admin. Div.

Kamal Rashid
Officer Operation Div.

Atif Alvi
AVP-II/I.T. Division

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 mitigate 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 anomalous 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 DDoS attacks, webscraping, and brute force attacks from ever taking place. Works with existing reactive anomaly 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.
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 allow 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 log for Application Security and Bot Defense.

Mohsin Ali Raho
AVP-II/ Admin. Div.

Kamal Rashid
Officer Operation Div.

Atif Alvi
AVP-II/I.T. Division

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 be 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 be able to configure a list of Allowed URLs for your web application
4. The WAF must be able to configure a list of Allowed Parameters for your web application
5. The WAF must be able to configure a list of Allowed Cookies for your web application
6. The WAF must be able to configure a list of Allowed HTTP Methods for your web application
7. The WAF must be capable of blocking specific list of HTTP methods
8. The WAF must be 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 be 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 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, etc...)
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 respond 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 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 File Type" List which may be seen in malicious requests, such as information leakage and remote code execution.

Mohsin Ali Raho
AVP-II/ Admin. Div.

Kamal Rashid
Officer Operation Div.

Atif Alvi
AVP-II/I.T. Division

32. The WAF shall come with a preconfigured list which users can add to.
33. The 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.
 - Info and Blocking Page configuration in Rule.
 - Transaction Outcome charts with filtering and drill-down capabilities.
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.

Mohsin Ali Raho
AVP-II/ Admin. Div.

Kamal Rashid
Officer Operation Div.

Atif Alvi
AVP-II/I.T. Division


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:

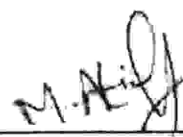
1. The WAF shall provide Public APIs Protection by loading the Customer-specific OpenAPI files, which are in Swagger format, to the platform to automatically create a security policy.
2. The WAF shall support JSON schema for user REST endpoints which can be uploaded to a JSON profile.
3. The WAF shall 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) - 1 (Help to Protect Web Application)

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

OPENING DATE: 07-08-21

OPENING TIME: 1130 hrs

ATTENDANCE (MEMBER PC)

NAME

FIRM

ATTENDANCE (REPS. OF BIDDERS)

① Innovative Integration (Pvt) Ltd

TOTAL BIDS ACCEPTED FOR EVALUATION

01

TOTAL BIDS REJECTED

REMARKS

SIGNATURE MEMBERS

Head - Fin Div. _____

Head - Admin Div. _____

Member - ID Div. _____

Date: _____



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) Ltd	FARAZ KHAN	0332-3000520	2nd Floor, CDA Building, G-Block, Wapda Road	Sargul Khan

Signature - Procurement Committee Members

Head of Administration

Chief Financial Officer

Chief Manager (IDBL)

(Handwritten signatures and initials over the procurement committee member lines)

<u>Buyer Record</u>		
S.No	Company Name	AMOUNT DEPOSITED
1	Innovative	300
Total		300



Stamp Vendor's Signature _____

16 JIN ZHENG

RECITALS

WHEREAS,

- A INNOVATIVE INTEGRATION (PVT.) LTD having resources, necessary infrastructure, approvals and skills to provide the Services to SINDH BANK LIMITED as detailed herein; Annexure A and
- B SNDB is a Banking company desirous of hiring the Services (defined in Annexure A);
- C SNDB has agreed to avail the Services from IIPL on the terms and conditions as set out in this Agreement.

NOW, THEREFORE, THIS AGREEMENT WITNESSETH and in consideration of the mutual covenants contained herein, the Parties do hereby agree, undertake and declare as under:

1. INTERPRETATION AND DEFINITIONS

1.1 In this Agreement, unless the context otherwise requires:

- References to Clauses and Appendices are references to clauses and appendices of this Agreement;
- Words importing one gender include the other gender;
- References to persons include bodies corporate, firms and unincorporated associations;
- The singular includes the plural and *vice versa*;
- References to all or any part of any statute or statutory instrument include any statutory amendment, modification or re-enactment in force from time to time and references to any statute include any statutory instrument or regulations made under it; The recitals to this Agreement shall form an integral part hereof; and
- The headings in this Agreement are for the purpose of reference only and shall be ignored in the interpretation of this Agreement.

1.2 In this Agreement, unless the context otherwise requires, the following terms shall have the following meaning:

“**Agreement**” is defined in the preamble;

“**Confidential Information**” is defined in Clause 5.1;

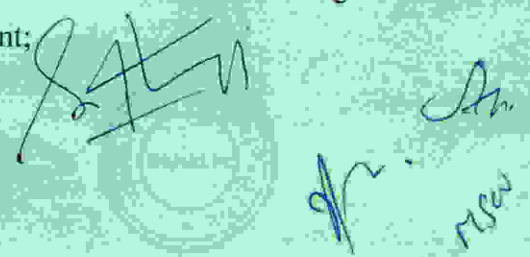
“**Force Majeure Event**” is defined in Clause 7.1;

“**Parties**” is defined in the preamble;

“**Party**” is defined in the preamble;

“**Payment Schedule**” means the aggregate charges for the Services calculated in accordance and set out in Annexure B of this Agreement; and

“**Services**” means the services to be provided by IIPL to SNDB under this Agreement as set out in detail under Annexure A of this Agreement;


The bottom right of the page contains several handwritten signatures in blue ink. A circular stamp of Sindh Bank Limited is partially visible, with the text 'Sindh Bank Limited' and 'Karachi' around a central emblem. The signatures appear to be from representatives of both parties.

2. TERM AND TERMINATION

- 2.1 All terms and condition of the tender documents will remain part of this agreement.
- 2.2 This Agreement shall be deemed to be effective from 02-07-2021 and shall remain in full force and effect until 02-07-2022, unless terminated earlier by either Party in terms of clause 2.3 below.
- 2.3 Contract agreement is extendable / renewable upto 2 years only on mutual written understanding on same terms & conditions and rates.
- 2.4 Any period within which Party shall, pursuant to this agreement, complete any action or task, shall be extended for a period equal to the time during which such Party was unable to perform such action because of Force Majeure.
- 2.5 This Agreement may be terminated by either Party by giving sixty (60) days prior written notice to the other Party. However, SNDB may forthwith terminate this Agreement with / without assigning any reason(s) or / and upon the occurrence of any one of the following events, without prejudice to any of its rights under this Agreement or any applicable laws:
- 2.6 Any petition being presented or a resolution being passed for liquidation (whether compulsory or voluntary, not being merely a voluntary liquidation, for the purposes of amalgamation or reconstruction) or insolvency or appointment of receiver of the assets or undertaking or any part thereof of IIPL; or
- 2.7 IIPL suspends its business or loses the right to undertake the Services business; or
- 2.8 IIPL suspends payment of its debts or admits (or is deemed to have admitted) its inability to pay its debts; or
- 2.9 IIPL engages in any conduct prejudicial to the image and goodwill of SNDB.
- 2.10 In the event of any material breach by either Party of its obligations hereunder, the breaching party shall have thirty (30) days from receipt of notice from the non-breaching party to rectify the breach after which time this Agreement shall stand terminated.
- 2.11 Upon termination, neither Party shall have any rights nor obligations to the other Party except as stated in this Agreement. However, all rights and obligations accruing prior to the date of termination shall continue to subsist.
- 2.12 If the either party engaged in corrupt or fraudulent practices in competing for or in executing the Agreement.
- 2.13 If, as the result of Force Majeure, the IIPL is unable to perform a material portion of the Services for a period of not less than thirty (30) days; and
- 2.14 If the either party, in its sole discretion and for any reason whatsoever, decided to terminate this Agreement.
- 2.15 If issued two (2) warning letters /emails by either party for unsatisfactory current performance.
- 2.16 Any notice, request or consent required or permitted to be given or made pursuant to this agreement shall be in writing. Any such notice, request or consent shall be deemed to have been given or made when delivered in person to an authorized representative of the Party to whom the communication is addressed, or when sent to such Party at the given address.
- 2.17 A party may change its address for notice by giving a notice to the other Party in writing of such change.
- 2.18 IIPL will not assign its job to anyone, except prior written permission of SNDB.

3. SERVICES / OBLIGATIONS OF INNOVATIVE INTEGRATION (PVT.) LTD

- 3.1 IIPL shall provide the Services as set out under Annexure A attached hereto.
- 3.2 IIPL shall perform the Services and carry out their obligations hereunder with all due diligence, efficiency and economy, in accordance with generally accepted professional standards and practices, and shall observe sound management practices, and employ appropriate technology and safe and effective equipment, machinery, materials and methods. IIPL shall always act, in respect of any matter relating to this Agreement or to the Services, as faithful advisers to the SNDB, and shall at all times support and safeguard the SNDB legitimate interests in any dealing with Sub-Suppliers or third Parties.
- 3.3 If the obligation of warranty period is not met or delayed, the repair etc. requirement on this account will be carried out by SNDB & the billed amount will be deducted from the performance security/ upcoming payment due to IIPL. Risk & subsequent cost to this effect if any will be liability of the IIPL and any subsequent expenses on the equipment will also be borne by the IIPL.

4. PAYMENT TERMS

- 4.1 In consideration of the covenants and agreements to be kept and performed by IIPL and for the faithful performance of this Agreement, SNDB shall pay and IIPL shall receive and accept (as full and final compensation for the Services furnished by IIPL under this Agreement) the payments as per Annexure B attached hereto.
- 4.2 It is expressly agreed between the Parties that the payment to be made by SNDB to IIPL for the Services rendered shall be fixed price during the entire duration of this Agreement without any revisions or negotiations in the price during the tenure of this Agreement. However after the tenure of this Agreement, the rates may be revised with mutual consent.
- 4.3 All or any payment(s) to be made by SNDB to IIPL shall be made subject to deduction of applicable taxes and levies.
- 4.4 IIPL and its Personnel shall be liable to pay such direct or indirect taxes duties, fees, and other impositions levied under the Applicable Laws, the amount of which deemed to have been included in Contract Price.
- 4.5 IIPL shall provide the performance security in the form acceptable to SNDB for the 10% of the tender value for the period of 1 Year from the date of Submission of performance security. In case IIPL does not fulfill its commitments, SNDB reserves the right to enforce the performance security.
- 4.6 SNDB shall be entitled to set off against and deduct and recover from any fees or other sums payable by SNDB to IIPL at any time, any tax, levy or other amount whatsoever which may be required to be deducted by order of any Court / Authority or under any law now existent or which may come into existence during the currency of this Agreement as well as any and all amounts which may be or become payable by IIPL to SNDB under this Agreement or pursuant thereto.
- 4.7 The payments to be made to IIPL in terms of this Clause 4 shall constitute the entire remuneration to IIPL in connection with the Services provided under this Agreement and neither IIPL nor its personnel shall accept any trade commission, discount, allowance or indirect payment or other consideration in connection with or in relation to this Agreement or to the discharge of the Services hereunder.

5. CONFIDENTIALITY

- 5.1 Any / All information concerning SNDB which is provided to IIPL and vice versa in connection with this Agreement ("Confidential Information"), shall be kept confidential by either Party, its affiliates, agents, advisors, directors, officers, or employees and, without the prior written consent of the other, each shall not:
- 5.2 distribute or disclose any of the Confidential Information in any manner whatsoever; or

2. TERM AND TERMINATION

- 2.1 All terms and condition of the tender documents will remain part of this agreement.
- 2.2 This Agreement shall be deemed to be effective from 02-07-2021 and shall remain in full force and effect until 02-07-2022, unless terminated earlier by either Party in terms of clause 2.3 below.
- 2.3 Contract agreement is extendable / renewable upto 2 years only on mutual written understanding on same terms & conditions and rates.
- 2.4 Any period within which Party shall, pursuant to this agreement, complete any action or task, shall be extended for a period equal to the time during which such Party was unable to perform such action because of Force Majeure.
- 2.5 This Agreement may be terminated by either Party by giving sixty (60) days prior written notice to the other Party. However, SNDB may forthwith terminate this Agreement with / without assigning any reason(s) or / and upon the occurrence of any one of the following events, without prejudice to any of its rights under this Agreement or any applicable laws:
- 2.6 Any petition being presented or a resolution being passed for liquidation (whether compulsory or voluntary, not being merely a voluntary liquidation, for the purposes of amalgamation or reconstruction) or insolvency or appointment of receiver of the assets or undertaking or any part thereof of IIPL; or
- 2.7 IIPL suspends its business or loses the right to undertake the Services business; or
- 2.8 IIPL suspends payment of its debts or admits (or is deemed to have admitted) its inability to pay its debts; or
- 2.9 IIPL engages in any conduct prejudicial to the image and goodwill of SNDB.
- 2.10 In the event of any material breach by either Party of its obligations hereunder, the breaching party shall have thirty (30) days from receipt of notice from the non-breaching party to rectify the breach after which time this Agreement shall stand terminated.
- 2.11 Upon termination, neither Party shall have any rights nor obligations to the other Party except as stated in this Agreement. However, all rights and obligations accruing prior to the date of termination shall continue to subsist.
- 2.12 If the either party engaged in corrupt or fraudulent practices in competing for or in executing the Agreement.
- 2.13 If, as the result of Force Majeure, the IIPL is unable to perform a material portion of the Services for a period of not less than thirty (30) days; and
- 2.14 If the either party, in its sole discretion and for any reason whatsoever, decided to terminate this Agreement.
- 2.15 If issued two (2) warning letters /emails by either party for unsatisfactory current performance.
- 2.16 Any notice, request or consent required or permitted to be given or made pursuant to this agreement shall be in writing. Any such notice, request or consent shall be deemed to have been given or made when delivered in person to an authorized representative of the Party to whom the communication is addressed, or when sent to such Party at the given address.
- 2.17 A party may change its address for notice by giving a notice to the other Party in writing of such change.
- 2.18 IIPL will not assign its job to anyone, except prior written permission of SNDB.

5.5 In the event that the receiving party received a request to disclose all or any part of the Confidential Information under the terms of a valid and effective subpoena or order issued by a Court of competent jurisdiction or by a government body, the receiving third party agrees to promptly notify the sending party of the existence, terms and circumstances surrounding such a report, prior to disclosing any such information, so that the sending party may seek an appropriate injunctive relief to safeguard the Confidential Information. If the receiving party is compelled to disclose any of the Confidential Information, it will disclose only that portion thereof which it is compelled to disclose and shall use its best efforts to obtain an order or other reliable assurance that confidential treatment will be accorded to the Confidential Information so disclosed. Confidential Information shall not include any information which:

5.6 has become generally available to the public through no fault or action of the receiving party; or

5.7 is in the possession of the receiving party prior to the date hereof, provided that such information is not known by the receiving party to be subject to another confidentiality agreement and further provided that such information was obtained independently and without the assistance of the sending party; or

5.8 is or becomes available to the receiving party on a non-confidential basis from any third party, the disclosure of which to the receiving party does not violate any contractual, legal or fiduciary obligation such third party has to the sending party.

5.9 Without limiting the generality of the foregoing, neither Party will publicly disclose the existence of or the terms of this Agreement without the prior written consent of the other. Furthermore, neither of the Parties will make any use of Confidential Information of the other Party except as contemplated by this Agreement; acquire any right in or assert any lien against the disclosing party's Confidential Information except as contemplated by this Agreement; or refuse to promptly return, provide a copy of or destroy such Confidential Information upon the request of the disclosing party, save for when destruction of such information would result in an impediment in the receiving party's performance of this Agreement. In such an event, the receiving party shall promptly inform the disclosing party in writing of its inability to do so, state clearly the reasons thereof and the time period in which the request will be complied with. The obligations of confidentiality herein shall remain in full force and effect during the life of this Agreement and shall survive the termination of this Agreement.

5.10 This clause 5.1, shall also survive after termination of this Agreement.

6. LIMITATION OF LIABILITY AND INDEMNIFICATION

6.1 In the event of any breach by IIPL of its obligations, warranties and / or responsibilities under this Agreement, IIPL shall hold SNDB, its subsidiaries, affiliates, officers, directors, employees and representatives harmless and indemnified from and against any and all losses (including without limitation any personal injury or death of any person), damages, claims, costs, liabilities, payments and obligations and all expenses (including without limitation reasonable legal fees) incurred, suffered, sustained or required to be paid, directly by or sought to be imposed upon SNDB or its subsidiaries, affiliates, officers, directors, employees and representatives.

6.2 IIPL shall maintain the highest professional code of conduct in its dealings. IIPL, its partners, employees, contractual staff etc. shall be responsible for any loss, delay or inconvenience caused to SNDB by an act, omission or negligence with respect to the Services and disclosure of Confidential Information or breach of any of the terms of this

Agreement. This is without prejudice to any other rights available to SNDB under this Agreement or any other applicable laws.

6.3 Without prejudice to the generality of the other provisions hereof, SNDB shall not be liable or responsible in any manner whatsoever in the event of any personal injury, including death caused to, including but not limited to the airline passengers, cabin crew, airline staff, airport staff or any other third party due to the provision of IIPL's Services or for losses, claims, damages whatsoever or howsoever caused, legal proceedings (if any), arising directly or indirectly in connection with the Services. Notwithstanding the generality of the above, SNDB expressly excludes liability for claimed consequential loss or damage or loss of profit, business, revenue, goodwill or anticipated savings.

6.4 This clause 6.1 shall also survive after termination of this Agreement

7. **FORCE MAJEURE**

7.1 Parties shall not be liable nor responsible for any non-performance of any obligation or losses arising out of any delay in or interruption of the performance of its obligations under this Agreement caused by any cause which is beyond the affected Party's reasonable control, including but not limited to, acts of God, act of governmental authority, act of the public enemy or due to war or terrorism, the outbreak or escalation of hostilities, riot, civil commotion, insurrection, labour difficulty in relation to a third party (including without limitation, any strike or other work stoppage or slow down), severe or adverse weather conditions, communications line failure, or other similar cause ("**Force Majeure Event**").

7.2 Upon the happening of a Force Majeure Event which continues for more than fourteen (14) days, SNDB may elect to terminate this Agreement with immediate effect or suspend the performance of this Agreement in whole or in part for the duration of the Force Majeure Event. In the event of termination, the Parties shall settle all outstanding amounts owing to the other immediately prior to the occurrence of such Force Majeure Event.

7.3 In the event that the Services or any part thereof is suspended on account of any Force Majeure Event, no fees shall be payable pursuant to this Agreement for the Services or any part thereof throughout the duration of such event but SNDB shall continue to pay in accordance with Clause 4 for all outstanding amounts and all other charges billed for the Services preceding the effective date of suspension.

8. **MEDIATION / ARBITRATION / DISPUTE RESOLUTION**

8.1 The Parties expressly agree that the dispute settlement procedure mentioned in this Clause 8 shall be a condition precedent to any action of law.

8.2 Any and every dispute, difference or question which may arise between the Parties to this Agreement shall be first settled by the Parties by an attempt at amicably settling the dispute through mutual negotiations.

8.3 In case the Mediation fails, the dispute shall be referred to Arbitration in accordance with the Arbitration Act 1940 and any applicable rules made there under for the time being in force, for the equitable decision of two joint arbitrators, one to be appointed by each of the Parties, and failing agreement between the arbitrators, to the decision of the umpire, to be appointed by the arbitrators before entering upon the reference. The award made by such arbitrators or the umpire, as the case may be, shall be final and binding on the Parties. The venue of the arbitration shall be Karachi and the arbitration proceedings shall be conducted in English language.

9. **GOVERNING LAW AND JURISDICTION**

9.1 Subject to Clause 8 above, this Agreement shall be governed by and construed in accordance with the laws of Pakistan. In relation to any legal action or proceedings arising out of or in connection with this Agreement, each of the Parties irrevocably submits to Civil/ Criminal jurisdiction of the competent Courts of Karachi, Pakistan.

MSW
NA

10. SEVERABILITY

- 10.1 If any provision of this Agreement is held invalid or otherwise unenforceable, the enforceability of the remaining provisions shall not be impaired thereby. In such case, the Parties shall make every effort to replace the ineffective provision with a new provision which has the same effect, or as approximate an effect as possible as the said provision.

11. THIRD PARTY RIGHTS

- 11.1 A person who is not a party to this Agreement has no right to enforce any term of this Agreement.

12. NOTICES

- 12.1 Any notice or other communication given or made or in connection with the matters contemplated by this Agreement shall be in writing and served to a Party at its address as specified in this Clause 12 (or any other address it has notified to the other Party in accordance with this Clause 12) as follows: by hand; by registered post; or by other electronic method of communication agreed in writing from time to time between the Parties.

- 12.2 Notices or communications sent by registered post will be deemed to have been served on the date that such mail is delivered or delivery is attempted. Notices or communications sent by fax will be deemed to have been served on the day of transmission if transmitted before 4.00pm in the time zone of receipt but otherwise on the next day. In all other cases, notices and communications will be deemed to have been served on the day when they are actually received.

- 12.3 Notices will be sent to:

Notices to Sindh Bank Limited will be sent to:

Attention: Information Technology Division
Address: 3rd Floor, Federation House, Clifton, Karachi.
Fax: 35870543

Notices to Innovative Integration (Pvt.) Ltd will be sent to:

Attention:
Address: 2nd Floor, KDLB Building, 58 West Wharf Road, Karachi
Fax: +922132314451

- 12.4 **Goods Faith:** The Parties undertake to act in good faith with respect to each other's rights under this agreement and to adopt all reasonable measures to ensure the realization of the objectives of this agreement.

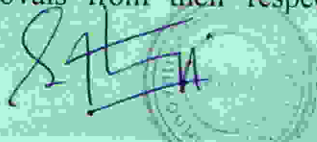
- 12.5 **Conflict of Interest:** IIPL shall hold the SNDB's interests paramount, without any consideration for future work, and strictly avoid conflict with other assignments or their own corporate interests.

13. AMENDMENTS

- 13.1 This Agreement may only be amended / modified in prior writing and signed by both Parties.

14. WARRANTIES AND REPRESENTATIONS

- 14.1 Both Parties warrant to each other that they have duly obtained all necessary consents and regulatory approvals from their respective competent authorities to enter into this Agreement.



- 14.2 Each Party represents and warrants to the other Party that neither the execution and delivery of this Agreement, nor the consummation of the transactions contemplated herein, will violate or conflict with: (a) its constitutional documentation; (b) any material provision of any agreement or any other material restriction of any kind to which it is a party or by which it is bound; (c) any material statute, law, decree, regulation or order of any governmental authority; or (d) any arrangement whereby it has not paid any collateral amounts to the other Party or any of its officer with regard to the award of contract hereunder or its performance.
- 14.3 Both Parties will use all reasonable care, skill and diligence in carrying out their obligations, duties and responsibilities under this Agreement.
- 14.4 Any and all intellectual property rights (legal and beneficial) accruing and attributable to a Party during the course of performance of its respective obligations under this Agreement shall vest in and with that Party.
- 14.5 Each Party represents and warrants to the other Party that there are no material actions, legal or administrative which adversely affects its ability to execute and perform its obligations under this Agreement.
- 14.6 IIPL acknowledges that SNDB has entered into this Agreement on the basis of the representations and undertakings made by IIPL throughout this Agreement.

15. USE OF NAMES, LOGOS AND REPORTS

- 15.1 Unless otherwise required by this Agreement, none of the Parties shall use, or disclose to third parties, the names, logos or reports of each other without the prior written consent of the concerned Party.

16. INTELLECTUAL PROPERTY

- 16.1 IIPL agrees it shall not use any of SNDB's names, logos, trademarks, trade secrets, copyrights, patents, designs and other intellectual property rights without the prior express written consent of SNDB.
- 16.2 Without prejudice to the other provisions of this Agreement, any infringement of intellectual property rights by IIPL in respect of any such items shall be deemed to be a material breach of a condition of this Agreement and shall entitle SNDB to terminate this Agreement forthwith upon prior written notice to IIPL.

17. COMPLIANCE WITH LAWS

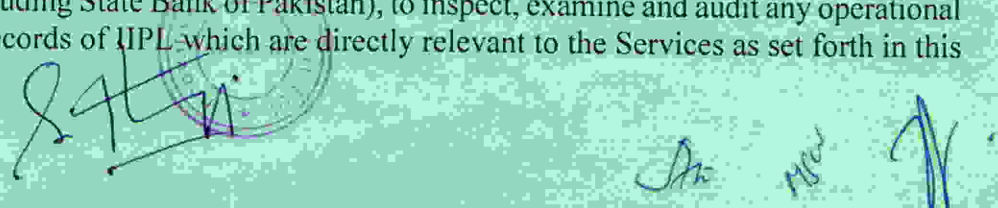
- 17.1 IIPL shall comply with all applicable laws, ordinances, regulations, and codes concerning IIPL's obligations as an employer with regard to the health, safety and payment of its employees, and identification and procurement of required permits, certificates, approvals, and inspections during the performance of this Agreement.

18. Anti- Money Laundering Requirement:

- 18.1 IIPL acknowledge that they do not violate any statutory/prudential requirement on anti money laundering or record keeping procedure as per existing laws/rules and regulations of locals as well as foreign jurisdiction.

19. RIGHTS TO AUDIT AND INSPECTION

- 19.1 IIPL agrees, upon prior written reasonable notice, to allow SNDB, its auditors and / or regulators (including State Bank of Pakistan), to inspect, examine and audit any operational and business records of IIPL which are directly relevant to the Services as set forth in this Agreement.

The bottom of the page features several handwritten signatures and stamps. On the left, there is a large, stylized signature in blue ink. To its right, there are several smaller, less distinct signatures and stamps, including what appears to be a circular official stamp and some handwritten initials or names.

20. UNAUTHORISED SOLICITATION OF EMPLOYEES

- 20.1 During the term of this Agreement neither Party shall without the prior written consent of the other Party solicit any person who at the commencement of this Agreement is a full time employee of such Party or engaged by the third party contractor providing services to such Party.

21. NON-AGENCY

- 21.1 In the conduct and performance of this Agreement, the Parties shall always be regarded as independent entities and not as partners, agents or employees of the other Party.

22. ASSIGNMENT AND SUB-LETTING

- 22.1 This Agreement is personal in nature, and cannot be assigned by IIPL without prior written permission of SNDB however, shall have the right to assign this Agreement to any third party without the consent of IIPL.
- 22.2 IIPL shall have no right to sublet or outsource all or any part of this Agreement or its obligations, rights and interests hereunder, to any third party without the prior written approval of SNDB.

23. TIME OF ESSENCE

- 23.1 IIPL understands that time is of the essence of this Agreement and it shall take all necessary steps to commence (and cause and ensure continuance of) the provision of the Services to SNDB, immediately commencing from the date of signing of this Agreement.

24. WAIVER

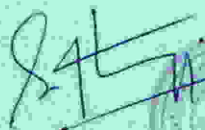
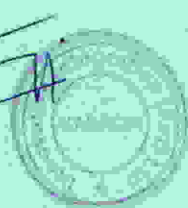
- 24.1 No waiver by either Party of any default by the other in the performance of any of the provisions of this Agreement shall be effective unless in writing duly executed by an authorized representative of the Party and no such waiver shall operate or be construed as a waiver of any other or further whether of alike or of a different character.

25. COUNTERPARTS

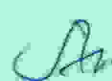
- 25.1 This Agreement shall be executed in two (2) counterparts, each of which shall be deemed an original and all of which together shall constitute one and the same instrument.

26. ENTIRE AGREEMENT

- 26.1 These terms and conditions constitute the entire agreement between the Parties and supersede all prior communications, proposals, understandings and agreements, written or oral between the Parties with respect to the subject matter of this Agreement.

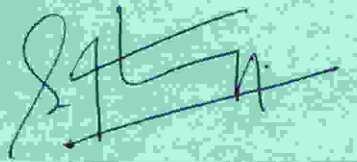









IN WITNESS WHEREOF the Parties, acting through their duly authorized representatives, have put their respective hands on this Agreement on the day month and year hereinabove mentioned.



For and on behalf of
Innovative Integration (PVT.) LTD,



For and on behalf of
Sindh Bank Limited

Name: SYED AKHTAR GHAZ
Designation: DIRECTOR
Seal:

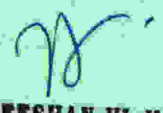


Name: SYED ATA HUSSAIN
Designation: HEAD OF IT
Seal:

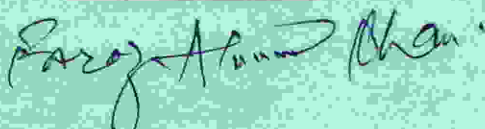
SYED ATA HUSSAIN
EVP Head Information Technology
SINDH BANK LIMITED
Head Office, Karachi.


Name: SYED AHMER GHAZ
Designation: CEO
Seal:



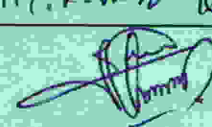
Name: 
Designation: SVP Information Technology
Seal: **SYED ZEESHAN-UL-HAQ**
SVP Information Technology
SINDH BANK LIMITED
Head Office, Karachi.

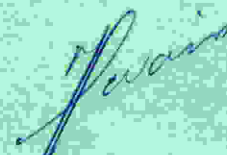
WITNESSES:

1. FARAZ AHMED KHAN


2. RIZWAN RAFIQ


WITNESSES:

1. M. Faran Khan


2. MUHAMMAD SARFARAZ WAKIL


MSW

ANNEXURE A

SERVICES / OBLIGATIONS OF

The SLA for Web Application Firewall (WAF-1)

- Innovative is responsible to maintain the equipment in proper working condition.
- Innovative will provide all the services based on severity level
- Innovative will be responsible to upgrade equipment with Software Updates released by the manufacturer related to the supplied equipment, if recommended.
- If a complaint is lodged during Coverage Hours, Innovative will respond to that request and provide solution based on severity level.
- Innovative will be responsible to undertake changes / additions in reconfiguration of supplied equipment. Any equipment not listed in this SLA will not be considered as part of this SLA.
- Innovative provide following services Planning, designing, deployments, upgrades and optimization to ensure a highly available, scalable, and secure infrastructure.
- Innovative will provide Onsite support for configuration hardware mentioned in Annex C.
- Innovative will provide facilitation in case of the RMA Process

[Handwritten signature]



[Handwritten signature]

[Handwritten signature]

[Handwritten signature]

ANNEXURE B

PRICE SCHEDULE

S.No.	Item	Unit Price	Qty	Amount (PKR)
1	Web application firewall (WAF-1) F5 AWAFF-i4600 (Specification as per tender document)	PKR7,130,053/-	2	PKR14,260,106/-
Total Amount (In PKR) Inclusive of All Taxes				PKR14,260,106/-

PAYMENT SCHEDULE

- Payment 50% on Delivery
- Payment 50% on Deployment

A handwritten signature in blue ink is written over a circular official stamp. The stamp contains the text "GOVERNMENT OF PUNJAB" and "OFFICE OF THE SECRETARY" around a central emblem.

A handwritten signature in blue ink.

A handwritten signature in blue ink.

A handwritten signature in blue ink.

ANNEXURE C

LIST OF EQUIPMENT & LICENSES

Below mentioned is the list of Equipment's covered under this SLA with Serial No, Model and Deployed Location.

S.N	Serial #	Model	Deployed Location	Feature / Licenses	Start Date	End Date
1	F5-XXXX-XXXX	F5-BIG-IP-i4600		BIG-IP i4600 Advanced Web Application Firewall		
				BIG-IP Service: Premium (Service Length 12 Months)		
2	F5-XXXX-XXXX	F5-BIG-IP-i4600		BIG-IP i4600 Advanced Web Application Firewall		
				BIG-IP Service: Premium (Service Length 12 Months)		

[Handwritten signature]

[Circular stamp]

[Handwritten signature]

[Handwritten signature]

Man

ANNEXURE D

ESCALATION MATRIX

ESCALATION MATRIX (AGENT – INNOVATIVE INTEGRATION)

Escalation 1st Level (response time 2 Hour)

Position	Name	Email	Office	Cell
Network Engineer	Saihaan Sanaullah	saihaan.sanaullah@innovativeintegration.net	32200013	+923323000797
Network Engineer	Hamza Shakoor	hamza.shakoor@innovativeintegration.net	32200013	+923323000523

Escalation 2ndLevel (response time 4 Hour)

Position	Name	Email	Office	Cell
Ammar Ahmed	Ammar Ahmed	ammar.ahmed@innovativeintegration.net	32200013	+923323000524
Account Manager	Faraz Khan	faraz.khan@innovativeintegration.net	32200013	+923323000526

Escalation 3rdLevel (response time 24 Hour)

Position	Name	Email	Office	Cell
Technical Director	Akhtar Ghazi	akhtar.ghazi@innovativeintegration.net	32200013	+923002533684

Signature


Signature

MSW

PURCHASE ORDER

PO No: 216

Date: 02-07-2021

M/s Innovative Integration (Pvt) Ltd,
2nd Floor, KDLB Building,
West Wharf,
Karachi.

Subject: Supply and Installation of Web Application Firewall (WAF-1)

Dear Sir,

With reference to the Tender Bid SNDB/COK/ADMIN/TD/1193/2021 dated 24-03-2021 for Supply and Installation of Web Application Firewall (WAF-1) at Sindh Bank Ltd, submitted by you. After detail review the Sindh Bank Ltd management is pleased to inform that your Tender Bid is accepted.

Kindly proceed as per tender document to supply the same at Head Office Sindh Bank. Further detail is as follows.

S.No	Product	Quantity	Unit Price PKR	Total Price (PKR) (Including All Taxes)
1	Web Application Firewall (WAF-1) F5 AWAFF -i4600 (Specification as per tender document)	02	7,130,053/-	14,260,106/-

Terms & Conditions

Payment Terms As per Agreement.
Delivery Within 8 weeks.
Taxes/Deduction Above prices are inclusive of all taxes.

Thanks,

Sarfaraz Waris
AVP-I/IT Division

M. Faraz Khan
AVP-II/I.T. Division

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

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

Riaz Ahmed
SVP/I.T Division

S. Ata Hussain
EVP/Head of IT

SINDH BANK LIMITED
HEAD OFFICE
3RD FLOOR, FEDERATION HOUSE,
ABDULLAH SHAH GHAZI ROAD,
CLIFTON, KARACHI-75600.

UAN : +92-111-333-225
PHONE : +92-21-35829320
+92-21-35829394
FAX : +92-21-35870543
WEB : www.sindhbank.com.pk

پولے این ۳۳۳-۱۱۱-۹۲
فون : ۳۵۸۲۹۳۲۰-۲۱-۹۲
۳۵۸۲۹۳۹۳-۲۱-۹۲
فیکس : ۵۴۳-۳۵۸۶۰۲۱-۹۲
ویب : www.sindhbank.com.pk

سندھ بینک لمیٹڈ
ہیڈ آفس: قیسری منزل، فیڈریشن ہاؤس،
عبداللہ شاہ غازی روڈ، کلٹن، کراچی۔ ۷۵۶۰۰

KALEEM
7/07/21



Innovative Integration (Pvt) Ltd.

E-mail: info@innovativeintegration.net

Website: www.innovativeintegration.net

Annexure "D"

Declaration of Fees, Commissions and Brokerage etc Payable by the Suppliers of Services Pursuant To Rule 89 Sindh Public Procurement Rules Act, 2010

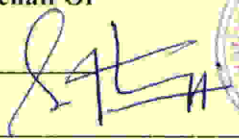
Innovative Integration (Pvt.) Ltd [the Supplier] hereby declares that it has not obtained or induced the procurement of any contract, right, interest, privilege or other obligation or benefit from Government of Pakistan (GoP) or any administrative subdivision or agency thereof or any other entity owned or controlled by it (GoP) through any corrupt business practice.

Without limiting the generality of the foregoing, [the Supplier] represents and warrants that it has fully declared the brokerage, commission, fees etc. paid or payable to anyone and not given or agreed to give and shall not give or agree to give to anyone within or outside Pakistan either directly or indirectly through any natural or juridical person, including its affiliate, agent, associate, broker, consultant, director, promoter, shareholder, sponsor or subsidiary, any commission, gratification, bribe, finder's fee or kickback, whether described as consultation fee or otherwise, with the object of obtaining or inducing the procurement of a contract, right, interest, privilege or other obligation or benefit in whatsoever form from GoP, except that which has been expressly declared pursuant hereto.

[The Supplier] certifies that it has made and will make full disclosure of all agreements and arrangements with all persons in respect of or related to the transaction with GoP and has not taken any action or will not take any action to circumvent the above declaration, representation or warranty. [The Supplier] accepts full responsibility and strict liability for making any false declaration, not making full disclosure, misrepresenting facts or taking any action likely to defeat the purpose of this declaration, representation and warranty. It agrees that any contract, right, interest, privilege or other obligation or benefit obtained or procured as aforesaid shall, without prejudice to any other right and remedies available to GoP under any law, contract or other instrument, be voidable at the option of GoP.

Notwithstanding any rights and remedies exercised by GoP in this regard, [the Supplier] agrees to indemnify GoP for any loss or damage incurred by it on account of its corrupt business practices and further pay compensation to GoP in an amount equivalent to ten times the sum of any commission, gratification, bribe, finder's fee or kickback given by [the Supplier] as aforesaid for the purpose of obtaining or inducing the procurement of any contract, right, interest, privilege or other obligation or benefit in whatsoever form from GoP.

For and On Behalf Of

Signature: 

Name: SYED AKHTAR SHAMS

NIC No: 42101-8266427-9



KARACHI OFFICE

2nd Floor, KDLB Building,
58 West Wharf Road, Karachi
Tel: +92 21 32311933, +92 21 32200013
Fax: +92 21 32314451

LAHORE OFFICE

Office No. 24, Al-Hafeez View,
1st Floor, 67/D-1, Gulberg III, Lahore
Tel: +92 42 35784491-94
Fax: +92 42 35784495

ISLAMABAD OFFICE

Office No. 305, 3rd Floor,
Emirates Tower, M-13, F-7 Markaz,
Islamabad
Tel: +92 51 2099155

3. SCOPE OF WORK / TECHNICAL SPECIFICATION

Sindh Bank requires Supply and Installation of Data Centre Web application firewall (WAF-1). 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 Two (02) 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: 650K L4 connections per second: 250K L4 HTTP requests per second: 1M Maximum L4 concurrent connections: 28M Throughput: 20 Gbps L4/L7
2	Hardware Offload SSL/TLS:	ECC+: 6.5K TPS (ECDSA P-256) RSA: 10K TPS (2K keys) 10 Gbps bulk encryption*
3	Software Compression:	6 Gbps
4	Software Architecture:	64-bit TMOS
5	On-Demand Upgradable:	YES
6	Processor:	One 4-Core Intel Xeon processor (total 8 hyperthreaded logical processor cores)
7	Memory:	32 GB DDR4
8	Hard Drive:	1 TB Enterprise Class HDD
9	Gigabit Ethernet CU Ports:	Optional SFP
10	Gigabit Fiber Ports (SFP):	8 SX or LX (sold separately)
11	10 Gigabit Fiber Ports (SFP+):	4 SR/LR (sold separately); optional 10G copper direct attach

Policy Management

- The WAF shall be able to automatically-built policies
- The WAF shall be able to manually accept false positives by simple means (check box)
- The WAF shall be able to define different policies for different applications
- The WAF shall be able to create custom attack signatures or events
- The WAF shall be able to customize Denial of Service policies
- The WAF shall be able to combine detection and prevention techniques
- The WAF shall have policy roll-back mechanism
- The WAF shall be able to do versioning of policies
- The WAF shall have a built-in real-time policy builder with automatic self-learning and creation of security policies
- The WAF shall have application- ready security templates for applications - eg Microsoft Sharepoint, OWA, ActiveSync, SAP, Oracle Applications/Portal, PeopleSoft, Lotus Domino for
- The WAF shall be capable of being restored to factory defaults
- The WAF shall have the ability to automatically detect server technologies and suggest adding the detected server technologies to the user's security policy.
- 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:
 - 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
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 (%uXXXX)
 - 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
 - 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 anomalous 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, webscraping, and brute force attacks from ever taking place. Works with existing reactive anomaly 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.
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 be 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 be able to configure a list of Allowed URLs for your web application
4. The WAF must be able to configure a list of Allowed Parameters for your web application
5. The WAF must be able to configure a list of Allowed Cookies for your web application
6. The WAF must be able to configure a list of Allowed HTTP Methods for your web application
7. The WAF must be capable of blocking specific list of HTTP methods
8. The WAF must be 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 be 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 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 respond 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 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.
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, Honeytrap 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