



ALLAHABAD BANK

**ADDENDUM-1 TO REQUEST FOR PROPOSAL
FOR
SUPPLY, INSTALLATION, CONFIGURATION, COMMISSIONING &
MAINTENANCE OF NEXT GENERATION FIREWALL APPLIANCES IN
ALLAHABAD BANK**

RFP Ref. No.: HO/DIT/NGFW/2018-19/116 dated: 01.10.2018

Addendum Date: 29-October-2018



Introduction

The Bank has floated the Tender Ref No HO/DIT/NGFW/2018-19/116 Dated: 01.10.2018 for Supply, Installation, Configuration, Commissioning & Maintenance of Next Generation Firewall Appliance in Allahabad Bank.

Pre Bid Queries Clarifications:

As per the terms of the RFP document, a pre-bid meeting was held on 06-10-2018, attended by the bidder's representatives.

As an outcome of the clarifications sought by the bidders at the pre-bid meeting and the queries received from the bidders through e-mail, this addendum dated 29-10-2018 to the RFP document is being issued herewith.

Other Amendments:

The Addendum covers clarifications to the queries raised by the bidders, few additional inclusions and amendments, which the Bank deems fit to be furnished to the bidders.

All other terms and conditions of the Tender document remain unchanged. Please treat this Addendum as an integral part of the Tender document issued.

No further queries pertaining to this Addendum will be entertained.

Chief Manager (IT)

Head Office, Kolkata



A. AMENDMENTS:

The following amendments have been made in this RFP, which the Bank deems fit to be furnished to the bidders.

1. Schedule of the RFP is amended as under:

Sl. No.	Items	Details
1.	Last Date for sale of RFP	12.11.2018 11:00 Hrs
2.	Last Date & Time of Submission of bids	12.11. 2018 15:00 Hrs
3.	Date and Time of Opening of Technical Bids	12.11.2018 16:30 Hrs
4.	Date and Time of Opening of Indicative Commercial Bids	To be notified subsequently to the technically qualified Bidders

2. Eligibility Criteria : The following eligibility criteria clauses only amended and rest other remains unchanged.

RFP Clause No	Existing Eligibility Criteria clause	Amended Eligibility Criteria clause
Eligibility Criteria Point No. 6	<p>A) Bidder should have supplied, Implemented and maintained similar Enterprise class firewall (which is successfully running) in at least two Scheduled Commercial Bank's Data Centre / Disaster Recovery Site (DRS) in India (excluding RRBs/ Co-operative Bank) with more than 2000 Branches within last five years as on date of submission of the Bid/ tender.</p> <p>OR</p> <p>B) Bidder should have been maintaining similar Enterprise class firewall (which is successfully running) in at least two Scheduled Commercial Bank's Data Centre / Disaster Recovery Site (DRS) in India (excluding RRBs/ Co-operative Bank) with more than 2000 Branches within last five years as on date of submission of the Bid/ tender.</p>	<p>A) Bidder should have supplied, implemented and maintained similar Enterprise class firewall (which is successfully running) in at least two Scheduled Commercial Bank's Data Centre / Disaster Recovery Site (DRS) in India (excluding Co-operative Banks) with more than 1000 Branches within last five years as on date of submission of the Bid/ tender.</p> <p>OR</p> <p>B) Bidder should have been maintaining similar Enterprise class firewall (which is successfully running) in at least two Scheduled Commercial Bank's Data Centre / Disaster Recovery Site (DRS) in India (excluding Co-operative Banks) with more than 1000 Branches within last five years as on date of submission of the Bid/ tender.</p>
Eligibility Criteria Point No. 4	<p>The bidder should be the Original Equipment Manufacturer (OEM) or certified / authorized agent of the solution offered.</p> <p>Further, Bidder should be an authorized partner with highest i.e. Tier-1 (Platinum/Gold) or equivalent, level of</p>	<p>The bidder should be the Original Equipment Manufacturer (OEM) or certified / authorized agent of the solution offered.</p> <p>Further, Bidder should be an authorized partner with highest i.e. Tier-1 (Platinum/Gold) or Tier-2 (Silver) or</p>



	<p>partnership with proposed OEMs for at least two years</p> <p>Note: (1) The bidder can be an authorized supplier of an OEM or OEM itself, but both OEM and its authorized supplier cannot bid simultaneously for the same item/product. (2) If a bidder submits a bid on behalf of the OEM, the same bidder cannot submit a bid on behalf of another OEM for the same item/product.</p>	<p>equivalent, level of partnership with proposed OEMs.</p> <p>Note: (1) The bidder can be an authorized supplier of an OEM or OEM itself, but both OEM and its authorized supplier cannot bid simultaneously for the same item/product. (2) If a bidder submits a bid on behalf of the OEM, the same bidder cannot submit a bid on behalf of another OEM for the same item/product.</p>
--	--	---

3. Payment Terms : The following payment term criteria clauses only amended and rest other remains unchanged.

RFP Clause No	Existing Eligibility Criteria clause	Amended Eligibility Criteria clause
Clause 42.1. Payment Terms (SI no. 1, 2 & 3)	<p>1) Delivery, Successful Installation and Acceptance of Hardware at each location(\$) - 60% of the Hardware cost</p> <p>2) After successful Go – Live of the Solution in each location - 30% of the Hardware cost Six months after successful Go Live of the solution in each location.</p> <p>3) Final payment will be released after one successful DR Drill - 10% of the Hardware Cost</p>	<p>1) 75% of the Hardware cost after Delivery, Successful Installation and Acceptance of Hardware at each location (\$)</p> <p>2) 10% of the Hardware cost after successful Go – Live of the Solution in each location.</p> <p>3) 15% of the Hardware Cost after six months after successful Go Live of the solution in each location, subject completion of one successful DR Drill..</p>

\$After successful completion of POC, if bank desires.

B. INCLUSIONS:

1. The following clause is to be included in “Form-3 :Minimum Technical and Functional Specification of Proposed Enterprise Class Next Generation Firewall”

The points that have been mentioned as “Y” (i.e, Complied) by the Bidder in Form-3 should be substantiated with sufficient proof and supporting documents like product sheet/ publicly available documents.

2. The following points are to be included in **Clause No 7.1. Broad Scope of Work:**



7.1.77. Bidder has to provide 1000 End Point Detection and Response Licenses for connecting 1000 concurrent user locations using laptop/PCs for Bank's Ultra Small Branches Project.

7.1.78. The proposed NGFW and Anti APT solution should be integrated with Bank's Active Directory services.

C. Pre Bid Queries Clarifications:

1. The clarifications/queries raised by the bidders are amended/ clarified in Annexure-I. Apart from these queries no other changes are done in the RFP.
2. **Responses towards all other queries /clarifications/clauses raised by the bidders may be treated as "RFP Requirement Stands".**



Annexure-1

Serial No	Page No	Clause ref	RFP text	Query Details	Bank's Response
1	143	Form-3 Sl.No.-5	The NGFW should have integrated Antivirus, IPS, Anti-malware, Anti-Botnet, IPSec VPN, Bandwidth Management, DPI, Application Control and user Control & awareness. Shall include during warranty, AMC & ATS for the appliance along with license & subscription for Gateway Antivirus, Antispam, spyware, Advance Threat prevention, Web / URL Filtering, content and application filtering, and IPS & on-premise sandboxing. License period will be counted after activation.	The NGFW should have integrated Antivirus, IPS, Anti-malware, Anti-Botnet, IPSec VPN, Bandwidth Management, DPI, Application Control and user Control & awareness. Shall include during warranty, AMC & ATS for the appliance along with license & subscription for Gateway Antivirus, spyware, Advance Threat prevention, Web / URL Filtering, content and application filtering, and IPS & on-premise sandboxing. License period will be counted after activation.	<i>The revised clause is as under:</i> Bidder may provide Antispam as an additional feature, if the feature is available in proposed NGFW solution or provided by OEM.
2	143	Form-3 Sl.No.--6	The proposed solution should be able to detect and prevent the BoT communication with Command & Control. Also the solution should have a Multi-tier engine to detect & prevent Command and Control IP/URL and DNS	The proposed solution should be able to detect and prevent the BoT communication with Command & Control.	<i>The revised clause is as under:</i> The proposed solution should be able to detect and prevent the BoT communication with Command & Control. Also the solution should have engine(s) to detect & prevent Command and Control IP/URL



					and DNS
3	145	Form-3 Sl.No.--32	The solution should provide with 12 no of 1 Gig copper ports, 4 no of 1 Gig SFP with SR and 4 no of 10 Gig SFP+ with SR ports. Solution should have 1 out of band management interface. Apart from this the solution should support 2 no of 1 Gig dedicated HA interfaces. The solution should support 40Gbps fiber port for future scalability.	<ol style="list-style-type: none"> 1. Please remove the 40 Gig interface requirement as this is favoring a particular OEM. 2. We would request the Bank to incorporate the need of 8 no of 10 Gig SFP+ interfaces, rather than 4 no of each as this will provide better flexibility. 	<p><i>The revised clause is as under:</i> The solution should provide with 12 no of 1 Gig copper ports, 4 no of 1 Gig SFP with SR and 4 no of 10 Gig SFP+ with SR ports or 12 no of 1 Gig copper ports and 8 no of 10 Gig SFP+ with SR ports. Solution should have 1 out of band management interface. Apart from this the solution should have separate dedicated HA interfaces. The solution should support 40Gbps fiber port for future scalability.</p>
4	145	Form-3 Sl.No.--33	The communication between all the components of Firewall system (firewall module, logging and policy management server and the GUI/WebUI console) should be encrypted and authenticated with SSL or PKI	As the bank has requested either on appliance or separate management of firewalls, this clause is not relevant for vendors who provide on-appliance management.	<p><i>The clarification is as under:</i> The bidder should provide a separate management solution either on appliance or server. The communication between management appliance/server and Firewall should be encrypted.</p>



5	146	Form-3 Sl.No.--53	<p>Proposed solution should be Next Generation Firewall and not an UTM (Unified Threat Management) system must support at least 4 Gbps of threat intelligence & threat prevention performance throughput with enabling firewall, application visibility and control, IPS, Anit-Botnet, Anti-virus, Anti-spyware & logging along with a mix of enterprise traffic of multi protocols like HTTP, FTP, DNS etc .</p> <p>The OEM should provide publically accessible Technical datasheets or provide latest 3 party report of quoted model or Prove quoted model having minimum required performance throughput at Bank's premises (Testing of quoted model) for substantiating the claim. All the expenses towards creating testing environment, required simulation tools etc should be born by the Bidder. Bank, at its own discretion may enable various security features on firewall at different point of time during contract period. In such cases if the threat Intelligence & threat prevention</p>	<p>The proposed solution will be a Next Generation Firewall and not an UTM (unified threat management) system, with a capability of supporting at least 3 Gbps of performance with Firewall, application control, IPS, Anti-Virus, Anti-spyware and logging enabled using 64 Kb HTTP transactions. In case of 64 KB transaction size is not specified, throughput should be based on "Real-world production conditions". The OEM should publish performance claims on public domain like websites, datasheets. Letter head performance claims will not be entertained. Allahabad Bank reserves the right to evaluate the performance based on Bank's traffic mix.</p>	<p><i>The revised clause is as under:</i></p> <p>Proposed solution should be Next Generation Firewall and not an UTM (Unified Threat Management) system must support at least 4 Gbps of threat intelligence & threat prevention performance throughput with enabling firewall, application visibility and control, IPS, Anit-Botnet, Anti-virus, Anti-spyware & logging along with a mix of enterprise traffic of multi protocols like HTTP, FTP, DNS etc (i.e Real-world production conditions) .</p> <p>The OEM should provide publically accessible Technical datasheets or provide latest independent 3rd party reports of quoted model or prove quoted model having minimum required performance throughput at Bank's premises (Testing of quoted model) for</p>
---	-----	-------------------	---	---	--



			throughput of the firewall goes above 80% of 4 Gbps (after enabling of all policies) then it will be considered as under performance. In case of underperformance, OEM has to upgrade or replace firewall/components to the next higher configuration without any additional cost to Bank.		substantiating the claim. All the expenses towards creating testing environment, required simulation tools etc should be borne by the Bidder. Bank, at its own discretion may enable various security features on firewall at different points of time during contract period. In such cases if the threat Intelligence & threat prevention throughput of the firewall goes above 80% of 4 Gbps (after enabling of all policies) then it will be considered as under-performance. In case of under-performance, OEM has to upgrade or replace firewall/components to the next higher configuration without any additional cost to Bank.
6	147	Form-3 Sl.No.--54	The solution should not have latency more than 10 microseconds	Kindly clarify the testing methodology for latency.	The clarification is as under: If this parameter is not provided in OEM product sheets and/or available publicly available documents,



					then during the contract period, in case of any performance issues, bidder should arrange for 3 rd party technical vendors or tools to prove the latency.
7	150	Form-3 Sl.No.--126	The solution should support keying hash value of a file so that if such file with same hash value is intercepted, the same gets blocked. The solution should also have third party intelligence feedback on hash values of malicious files.	Requested for removal.	<i>The revised clause is as under:</i> The solution should support keying/ uploading hash value of a malicious file so that if such file with same hash value is intercepted, it will get blocked. The uploading of hash values may be automated or manual. The solution should also get automated intelligence feedback on hash values of malicious files from its regular signature.
8	151	Form-3 Sl.No.--139	The proposed solution should have a Multi-tier engine i.e. Detect and Prevent command, Control IP, URL & DNS	Requested for removal.	<i>The clause is revised as under:</i> The proposed solution should have engine(s) i.e. Detect and Prevent command, Control IP,



					URL & DNS
9	151	Form-3 Sl.No.--143	Anti-virus scanning should support proactive and stream mode	Requested for removal.	<i>The clause is revised as under:</i> Anti-virus scanning should support proactive or stream mode or both
10	151	Form-3 Sl.No.--145	Solution should give information related to Performance impact and confidence level of protections while creating profiles	Requested for removal.	<i>The clause is revised as under:</i> This feature may be treated as optional. If, the proposed appliances are having the said feature, Bidder should provide the same with no additional cost to the Bank.
11	153	Form-3 Sl.No.--191	Solution should multiple deployment options like Inline/ Tap	Inline/ Tap-- is it or Condition? Please clarify.	RFP stands. The Solution should support multiple deployment options Inline and Tap. Bank will have option to install the way it wants
12	153	Form-3 Sl.No.--193	Endpoint Detection and Response	Requested for removal.	<i>The Clarification is as under:</i> Bank intends to connect 1000 end points under Ultra Small Branch Project through Internet. Endpoint Detection and Response should work in the Firewall. Bidder also has



					to integrate Active Directory (AD) with the Firewall.
13	154	Form-3 Sl.No.--206	The solution should be able to identify malware present in file types and web objects such as (JPEG, doc, docx, exe, gif, hip, htm, , pdf, png, ppsx, ppt, pptx, qt, rm, rtf, swf, tiff, url, vbs, vcf, xls, xlsx. etc.) and be able to quarantine/ remove them.	Requested for removal.	<i>The revised clause is as under:</i> The solution should be able to identify malware present in majority of file types and web objects such as (JPEG, doc, docx, exe, gif, hip, htm, , pdf, png, ppsx, ppt, pptx, qt, rm, rtf, swf, tiff, url, vbs, vcf, xls, xlsx. etc.) and be able to quarantine/ remove them. In case any of the file type(s) are currently not supported, those which are subsequently supported by the proposed OEM should also provide & upgrade to the Bank at no additional cost during the contract period.
14	154	Form-3 Sl.No.--208	The solution should be able to scan & find for unknown threats in executable, archive files ,documents, Java Applet, (jar and class), JAVA and flash specifically: Microsoft office, 7z ,cab, csv, pdf, potx, pps, ppsm, ppsx,	Requested for removal.	<i>The revised clause is as under:</i> The solution should be able to scan & find unknown threats in executable, archive files ,documents, Java Applet, (jar



			<p>ppt, pptm, pptx, rar, rtf, scr, swf, tar tgz, docm, docx, dot, dotm, dotx, jar, xla, xlsb, xlsx, xlt, xltm, xltx, xlw, zip, Android Application Package (APK) etc.</p>		<p>and class), JAVA and flash specifically: Microsoft office, 7z ,cab, csv, pdf, potx, pps, ppsm, ppsx, ppt, pptm, pptx, rar, rtf, scr, swf, tar tgz, docm, docx, dot, dotm, dotx, jar, xla, xlsb, xlsx, xlt, xltm, xltx, xlw, zip, Android Application Package (APK) etc. In case any of the file type(s) currently not supported , those which are subsequently supported by the proposed OEM should also provide & upgrade to the Bank at no additional cost during the contract period.</p>
15	155	Form-3 Sl.No.--216	<p>In case there is no antivirus signature available for malware, solution should have the ability to exfiltrate data about the malware and share it with the antivirus solution providers.</p>	Requested for removal.	<p>The revised clause is as under: This feature may be treated as optional. If, the proposed appliances have the said feature, Bidder should provide the same with no additional cost to the Bank.</p>



16	155	Form-3 Sl.No.--226	Appliance may be supplied with minimum 2x10GbESFP/SFP+	Appliance may be supplied with minimum 4x10/100/1,000	The revised clause is as under: Appliance may be supplied with minimum 4 x 10/100/1000, However 2 x 10 Gbps SFP/SFP+ is preferable.
17	155	Form-3 Sl.No.--213	The solution should be able to block the call back tunnel including fast flux connections / Domain Generation Analysis (DGA).	Requested for removal.	The revised clause is as under: The solution should be able to block the call back tunnel including fast flux connections or Domain Generation Analysis (DGA) or equivalent
18	155	Form-3 Sl.No.--227	Automatic signature updates in less than 30 min for all new malware detected anywhere in the world	1. Is the bank ready for 30 mins window of attack surface? 2. This should be minimal to 5 mins.	The revised clause is as under: Automatic signature updates in less than 5 min for all new malware detected anywhere in the world
19	155	Form-3 Sl.No.--229	Solution should have end protection solution to secure mobile devices/laptops/IPads/Smartphone such variants of android, iOS, Windows based OS	Request for removal	The revised clause is as under: Solution should have end protection solution to secure mobile devices/laptops variants of Windows based OS. However, during the



					contract period OEM supports the IOS / Android based devices, Bidder should provide the same upgrade to the Bank at no additional cost.
20	18	Eligibility Criteria Sr No. 6	<p>A) Bidder should have supplied, Implemented and maintained similar Enterprise class firewall (which is successfully running) in at least two Scheduled Commercial Bank's Data Centre / Disaster Recovery Site (DRS) in India (excluding RRBs/ Co-operative Bank) with more than 2000 Branches within last five years as on date of submission of the Bid/ tender.</p> <p>OR</p> <p>B) Bidder should have been maintaining similar Enterprise class firewall (which is successfully running) in at least two Scheduled Commercial Bank's Data Centre / Disaster Recovery Site (DRS) in India (excluding RRBs/ Co-operative Bank) with more than 2000 Branches within last five years as on date of submission of the Bid/ tender.</p>	<p>Request to amend the clause as:</p> <p>A) Bidder should have supplied, Implemented and maintained similar Enterprise class firewall (which is successfully running) in at least ONE Scheduled Commercial Bank's Data Centre / Disaster Recovery Site (DRS) / SOC in India (excluding RRBs/ Co-operative Bank) with more than 1000 Branches OR at least ONE GOVT / PSU Organization within last five years as on date of submission of the Bid/ tender.</p> <p>OR</p> <p>B) Bidder should have been maintaining similar Enterprise class firewall (which is</p>	Pl refer Amendments section of this addendum.



				successfully running) in at least ONE Scheduled Commercial Bank's Data Centre / Disaster Recovery Site (DRS) / SOC in India (excluding RRBs/ Co-operative Bank) with more than 1000 Branches or at least one GOVT / PSU Organization within last five years as on date of submission of the Bid/ tender.	
21	17	Eligibility Criteria Sr No. 4	<p>The bidder should be the Original Equipment Manufacturer (OEM) or certified / authorized agent of the solution offered.</p> <p>Further, Bidder should be an authorized partner with highest i.e. Tier-1 (Platinum/Gold) or equivalent, level of partnership with proposed OEMs for at least two years</p> <p>Note: (1) The bidder can be an authorized supplier of an OEM or OEM itself, but both OEM and its authorized supplier cannot bid simultaneously for the same</p>	<p>To ensure maximum participation, amend the clause as:</p> <p>The bidder should be the Original Equipment Manufacturer (OEM) or certified / authorized agent of the solution offered.</p> <p>Further, Bidder should be an authorized partner with with highest or 2nd highest i.e. Tier-1 (Platinum/Gold) or equivalent OR Tier 2 Or Equivalent level of partnership with proposed OEMs as on</p>	Pl refer Amendments section of this addendum.



			item/product. (2) If a bidder submits a bid on behalf of the OEM, the same bidder cannot submit a bid on behalf of another OEM for the same item/product.	date of bid submission.	
22	147	Form3- Sr No-62	Solution should provide 240 GB for log storage. In addition, it should provide the ability to transfer logs to SIEM solutions and external Syslog servers.	Considering the fact that the logs needs to be stored in the NGFW appliance in case the central logging is not available, the maximum capacity of the SSD drives available is 480GB. Request to modify the clause as " <u>Solution should provide 480 GB for log storage. In addition, it should provide the ability to transfer logs to SIEM solutions and external Syslog servers.</u> "	<i>The revised clause is as under:</i> Solution should provide minimum with 240 GB for log storage. In addition, it should provide the ability to transfer logs to SIEM solutions and external Syslog servers.
23	151	Form3- Sl.No -153	Firewall Real-time Monitoring, Management & Log Collection (with Storage) should not be distributed to more than one server / appliance	Clarify whether the APT solution and NGFW solution needs to be managed from the single management.	<i>The clarification is as under:</i> Bidder may provide separate single/multiple management appliance(s) or server & software based solution(s) to manage both NGFW solution and the APT solution.



24	77	Clause 42.1. Payment Terms	<p>Delivery, Successful Installation and Acceptance of Hardware at each location(\$) - 60% of the Hardware cost</p> <p>After successful Go – Live of the Solution in each location - 30% of the Hardware cost Six months after successful Go Live of the solution in each location.</p> <p>Final payment will be released after one successful DR Drill - 10% of the Hardware Cost</p>	<p>Request the payment terms for hardware to be amended as:</p> <p>Delivery at each location- 70% of the Hardware cost</p> <p>Successful Installation and Acceptance of Hardware 15%</p> <p>After successful Go – Live of the Solution in each location - 10% of the Hardware cost</p> <p>Six months after successful Go Live of the solution in each location. Final payment will be released after one successful DR Drill - 5% of the Hardware Cost</p>	Pl refer Amendments section of this addendum.
25	144	Form3- Sl.No - 17	The Bidder should ensure that there is SPOC from OEM throughout the project period and OEM must provide 24 X 7 X 365 technical support. The OEM must provide the dedicated login credentials to Allahabad Bank with highest level permissions to search knowledge base, downloading of the patches, documents and to manage	Clarify the credentials and scope of the SPOC from the OEM desired by Allahabad bank for effective project completion.	The clarification is as under: OEM must provide 24 X 7 X 365 technical support to Bank. The OEM must provide the dedicated login credentials to Allahabad Bank with highest level permissions to search knowledge base, downloading of the patches, documents and



			the device. Allahabad Bank should be able to raise tickets directly to OEMs.		to manage the device. Allahabad Bank should be able to raise tickets directly to OEMs.
26	23	7.1.18 Broad Scope of Work	The bidder should be responsible for de-commissioning of existing devices at DC and DR i.e, replacing the existing Firewall with the new firewall in such a way that there is no impact on business continuity. If need be, the successful Bidder may arrange for resources having expertise in existing Firewall to ensure the same.	Bank may permit to operate from DR location during the firewall change.	RFP Stands. However, Bank may decide to commission new Firewall during DR Drill.
27	22	7.1.9-Broad Scope of Work	Solution (Hardware & software) should not be due for declaration of End-of-Sale within 2 years from last date of submission of Bid.	Both the statements contradict with respect to period. Request Bank to specify correct period.	The revised clause is as under: Solution (Hardware & software) should not be due for declaration of End-of-Sale within 3 years from last date of submission of Bid.
28	27	7.1.72- Broad Scope of Work	Bidder has to provide for required hardware/ software/ third party tools to support archiving requirements of the bank for the entire contract period.	Request bank to clarify on this point.	The clarification is as under: Bank would require to archive the logs as well as configuration files. The bidder has to provide required hardware/ software/ third



					party tools, if there is need for the same
--	--	--	--	--	--

Responses towards all other queries /clarifications/clauses raised by the bidders may be treated as “RFP Requirement Stands”.

****END OF DOCUMENT****

