

UCO BANK
Department of Information Technology

Request for Proposal (RFP) For Management, Maintenance and Monitoring of Network Devices and Link at Branches, DC, DR and other offices of the bank RFP REF NO: UCO/DIT/NW/465/2016-17 Date: 06/09/2016
Pre-Bid Responses/ Clarifications to Queries raised by the Bidder(s), Amendments, Addendums and Corrigendum's

SL No	Page no	Clause	Clause as per RFP	Description of Query/Clarification sought by Bidder	Bank Response
1	21	Part IV - Scope of Work	The bidder is expected to liaison with the third party, government authorities etc.	What is all about the Government authority permissions is it for the new infra or existing infra?	New and existing infra both
2	21	Part IV - Scope of Work Sub clause: Network Connectivity at branches	120++ Branches have MPLS backed up by MPLS link by alternate service provider.	Who is MPLS service provider for 120 + branches for backup link?	M/s TCL, M/s Reliance & M/s Sify.
3	22	Part IV - Scope of Work Sub clause: Network Connectivity at branches	xi) ATM switch is connected from BDC and KDC through MPLS to Euronet Mumbai and Chennai datacentre using 4 nos. of TCL Link and 3 nos. of Sify Link should managed by the bidder xii) 4 nos. of international branches are connected through M/S TCL and M/S Sify MPLS Link with Data Centre.	Is it TCL & Sify MPLS is common for International connectivity & ATM Switch Connectivity?	M/s TCL and M/s Sify both are providing link for International branches and ATM switch connectivity. But MPLS network for International branches and ATM switch both network are different.
4	22	Part IV - Scope of Work	As per the service the bidder has to deploy specialized onsite network team at Bank DC and DR and 20 ZO locations (Annexure – H) to manage the network with Network Management tools to be provided by Bank.	Who manage the Network Management Tool?	M/s HPE will manage the Network Management Tool. AMC & ATS for Network Management Tool will provide by M/s HPE However Successful bidder should use the tool to manage the Network.
5	23	Part IV - Scope of Work 4.2 baselines	Service delivery model	Is the service Provider SLA in lined with Bidders SLA?	Service Provider will maintain the similar uptime.
6	24	Part IV – Scope of Work 4.4 WAN Network Monitoring	vii) As Bank is going for commissioning of 2nd service provider's MPLS link/VSAT	we have around 1500 branches running on ISDN/CDMA backup connectivity how many circuits we are migrating per Year/Month/Week to MPLS or VSAT	Depending upon feasibility/ commissioning of links from alternative service provider.
7	25	Part IV – Scope of	ix) Provide information &	Does the existing tool have a capability	

		Work 4.5 Network Management Service	recommendations to Bank on the links and devices which are over utilized.	to capture the BW utilization etc.?	Yes
8	25	Part IV – Scope of Work 4.5 Network Management Service	xii) Preparing the network diagram and updating it on a continual basis	Do we have a Network Diagram for existing setup?	Yes
9	28	4.12 Uptime maintenance		Do we have our network device Level redundancy available	At DC & DR site.
10	29	4.15 Configuration management		Redesign will be part of support scope or it will be a new project.	Redesign of network for support service and it will be for new project also in future.
11	78	WAN Optimization		Can we provide WAN Optimization as a service?	NO
12	22	Part IV - Scope of Work Sub clause: Network Connectivity at branches	xi) ATM switch is connected from BDC and KDC through MPLS to Euronet Mumbai and Chennai data centre using 4 nos. of TCL Link and 3 nos. of Sify Link should managed by the bidder xii) 4 nos. of international branches are connected through M/S TCL and M/S Sify MPLS Link with Data Centre.	Onsite support for International location is it with current scope of work?	Yes, in case of any network device failure which is under bidder support.
13			New Branch Roll out	Any Projection for New Branch roll out (Yearly /Monthly/ Weekly)	Any time in year.
14				Any ITSM tool used currently?	NO
15	35	4.64	Management of network equipment on site and providing L1/L2/L3 support for fault diagnostic for both software and hardware	L3 support was mentioned in the RFP but there is no L3 count the resource count.	L3 support is required as and when onsite or over phone to maintain desire uptime.
16			Helpdesk support Zonal Office	Clarify the Zonal office help desk support do we have a separate support team for Zonal office?	Bidder should provide one seat at each 20 identified ZOs for branch support. Besides, on call basis manpower should be available to support branches network during any network problem in the site. Successful Bidder to deploy adequate manpower at filed level to ensure the desired uptime.
17	24	4.3 On site Manpower Assignment	v) On-going training program for quarterly basis.	Need clarity on this	Clause Deleted. Reference: Part IV, Point 4.3 (V)
18	25	Part IV – Scope of Work 4.5 Network Management Service	x) Periodic updates, audits for network device inventory.	Please mention the frequency of the Audit and Inventory update interval	Quarterly basis.
19			Record and implement Service Requests as requested by Bank.	We assume that banks existing Service Desk tool will be extended to bidder for call management (Incident/ Service request) and change management Process. Please confirm	Yes

20		General		Please confirm if bidder may deploy a combination of it payroll resource and partner resource for Service.	Yes. Should not be any deviation from labour law of our country .
21	25	4.6 Core Networking	xii) Logs and backup management	Are you using any tool for automated logs and configuration backup management in the existing scenario?	No.
22	25	4.6 Core Networking	xv) Network Software Management	We understand that you are asking bidder to manage NMS tools. Please confirm if our understanding is correct.	NO. M/s HPE will manage the Network Management Tool. AMC & ATS for Network Management Tool will provide by M/s HPE. However Successful bidder should use the tool to manage the Network.
23			Network recovery should be automatically from primary to Secondary and vice-versa.	Is the existing configuration capable of automatic failover from primary to secondary?	Yes
24			Migration of IPv6 network at internet, if required.	This is a complete migration activity. Request you to remove this from FMS scope	Please refer sl. No. 8 in corrigendum
25	28	4.11 Managing and Supporting Network at help Desk level	ii) The support at help desk level should be available during business hours (8.00AM to 8.00PM)for all 20 ZO's. iv) The help desks should be manned by dedicated manpower as per the details given at clause 4.3.	In the onsite manpower assignment table you have asked 20 manpower (one at each location) for providing support at Zonal offices. One engineer/ ZO will not be able to cover 12 hrs. support on regular basis. Can we consider 9 hrs. (9 AM - 6 PM) onsite support and 3 hrs. (8AM -9 AM & 6 PM-8 PM) remote support from DC for all ZO s?	The support at help desk level should be available during business hours (10.00AM to 7.00PM)for all 20 ZO's.
26	28	4.11 Managing and Supporting Network at help Desk level	vii) The Successful bidder is responsible to resolve the problem within the stipulated time schedule referred by any of the following: i. The network trouble tickets generated in the EMS tool ii. Telephonic information iii. E-mail information etc.	i) Scope is only related with IPv6 implementation or Liaison with Service Provider for IPv6 Block also. ii) For IPv6, server should have dual stack IPv4 & IPv6 implemented. Is IPv6 implemented in current setup?	Please refer sl. No. 8 in corrigendum
27	35	4.57	IP scheme management including IPv6.	Is KDC, BDC and branch IPv6 migration also is scope?	Please refer sl. No. 8 in corrigendum
28	65	Annexure G	5.Routers should have at least 1 open slots for V.35 serial interfaces	Please confirm Serial Interface required from day one?	For Type A router in Annexure G & J serial card required from day one.
29	9	1.2 Submission of bid	1.2.7 Incomplete bids or bids not conforming to the terms and conditions are liable for rejection by the Bank	Incomplete bids or bids not conforming to the terms and conditions and the deviations submitted along with this bid, are liable for rejection by the Bank	Clause stands as per RFP.
30	10	1.2 Submission of bid	1.2.14 The bidder is required to guarantee that exchange rate fluctuations, changes in import duty and other taxes will not affect the Rupee value of the commercial bid over the price validity period	The bidder is required to undertake guarantee that exchange rate fluctuations, changes in import duty and other taxes will not affect the Rupee value of the commercial bid over the price validity period	Clause stands as per RFP.

				If there is any change in the exchange rate during contract period, recommended to consider at the prevailing rate at the time of billing/payment.	
31	11	1.2 Submission of bid	1.2.23 The Bank expects the Selected bidder to adhere to the terms of this RFP document and would not like or accept any deviations to the same.	The Bank expects the Selected bidder to adhere to the terms of this RFP document and would not like or accept any deviations to the same.	Clause stands as per RFP.
32	11	1.2 Submission of bid	1.2.25 The Bidders will have to guarantee availability of comprehensive support of entire infrastructure including future upgrades at no additional cost to the bank for the solution for the contract period.	The Bidders will have to undertake guarantee availability of comprehensive support of entire infrastructure including future upgrades at mutually agreed no additional cost to the bank for the solution for the contract period.	Clause stands as per RFP.
33	13	1.5 Rejection of bid	1.5.5 Bidder should comply with all the points mentioned in the RFP.	Bidder should comply with all the points mentioned in the RFP, except for the deviations submitted along with this bid.	Clause stands as per RFP.
34	16	1.17 Acceptance of terms	A Recipient will, by responding to Bank RFP, be deemed to have accepted the terms as stated in the RFP	A Recipient will, by responding to Bank RFP, be deemed to have accepted the terms as stated in the RFP, except for the deviations submitted along with this bid	Clause stands as per RFP.
35	17	1.22 Indemnity	The bidder shall indemnify the Bank and be liable for any loss or damage suffered by the Bank due to malfunctioning of the system as supplied and installed by them.	Liability: The bidder shall indemnify the Bank and be liable for any loss or damage suffered by the Bank due to malfunctioning of the system as supplied and installed by them. The aggregate total liability including for SLA LD or any other penalty of the selected bidder under this RFP shall not exceed the total cost of the order value.	Clause stands as per RFP.
36	26	4.8 Supply, installation, configuration and maintenance of Equipment	xiii) In case there is a cost incurred to the bank due the wrong configuration of network equipment at any location, the same will be borne by the Successful Bidder.	In case there is a cost incurred to the bank due the wrong configuration of network equipment at any location, the same will be borne by the Successful Bidder provided such configuration is due to successful bidder' act .	Clause stands as per RFP.
37	31	4.20 Covenant of the bidder	Depending on the sensitivity and criticality of the services or data provided, Bank will consider commissioning or requesting a review	delivery and audit team to confirm. This looks onerous as bank intends to audit our internal control structure	Clause stands as per RFP.

			of Bidder's internal control structure for ensuring that any confidential/restricted/internal information of the Bank is maintained securely.		
38	38	5.5 Price	The Selected bidder is required to guarantee that exchange rate fluctuations, changes in import duty and other taxes will not affect the Rupee value of the commercial bid, over the validity period of the bid.	The Selected bidder is required to undertake guarantee that exchange rate fluctuations, changes in import duty and other taxes will not affect the Rupee value of the commercial bid, over the validity period of the bid.	Clause stands as per RFP.
39	39	SLA		the up time requirements seem very high.	Clause stands as per RFP.
40	41	5.8 Liquidated damage	Any delay in delivery/installation/commissioning/shifting/upgradation of the link/device/equipment/solution beyond the stipulated time period as per clause no. 5.3, Bank will charge penalty at 1 % of the order value for that link/device/equipment/implementation cost per week or part thereof, subject to a maximum of 10%.	Any delay in delivery/installation/commissioning/shifting/upgradation of the link/device/equipment/solution beyond the stipulated time period as per clause no. 5.3, Bank will charge penalty at 0.5 + % of the order value for that link/device/equipment/implementation cost per week or part thereof, subject to a maximum of 5 10 % of the order value for that link/device/equipment/implementation cost	Clause stands as per RFP.
41	41	5.8 Liquidated damage	If Bidder fails to commission the link as per feasibility report (this includes change of media) 10% of the link cost will be deducted from payment of other link or from Performance Bank Guarantee and bank will place the order to any other selected bidder	If Bidder fails to commission the link as per feasibility report (this includes change of media) 10% of the link cost will be deducted from payment of other link or from Performance Bank Guarantee and bank will place the order to any other selected bidder	Clause stands as per RFP.
42	42	5.10 completeness of project	The project will be deemed as incomplete if the desired objectives of the project as mentioned in Section "Scope of Work" of this document are not achieved.	The project will be deemed as incomplete if the desired objectives of the project as mentioned in Section "Scope of Work" of this document are not achieved, due to selected bidder's acts or omission.	Clause stands as per RFP.
43	42	5.11 Acceptance Testing	The provisioned items will be deemed accepted only on successful acceptance of those products and the vendor would need to provision insurance of those items till successful acceptance.	The provisioned items will be deemed accepted only on successful acceptance of those products and the vendor would need to provision insurance of those items till successful acceptance.	Clause stands as per RFP.
44	42	5.11 Acceptance Testing	The Bank have the right to reject the 'Vendor Supplied Link' and to seek free replacement of the link till the completion of acceptance test and	The Bank have the right to reject the 'Vendor Supplied Link' and to seek free replacement of the link till the completion of acceptance test and	Clause stands as per RFP.

			obtaining final acceptance certificate from the Bank	obtaining final acceptance certificate from the Bank	
45	43	5.12 Order cancellation	Vendor should be liable under this section if the contract/ purchase order has been cancelled in case sum total of penalties and deliveries equal to exceed 10% of the TCO.	Vendor should be liable under this section if the contract/ purchase order has been cancelled in case sum total of penalties and deliveries equal to The maximum aggregate liability of the vendor under the RFP shall not exceed 10% of the TCO.	Clause stands as per RFP.
46	43	5.12 Order cancellation	In case of cancellation of order, any payments made by the Bank to the Vendor would necessarily have to be returned to the Bank, further the Vendor would also be required to compensate the Bank for any direct loss suffered by the Bank due to the cancellation of the contract/purchase order and any additional expenditure to be incurred by the Bank to appoint any other Vendor.	In case of cancellation of order, any payments made by the Bank to the Vendor would necessarily have to be returned to the Bank, further the Vendor would also be required to compensate the Bank for any direct loss suffered by the Bank due to the cancellation of the contract/purchase order and any additional expenditure to be incurred by the Bank to appoint any other Vendor.	Clause stands as per RFP.
47	44	5.13 Indemnity	Vendor shall indemnify, protect and save the Bank and hold the Bank harmless from and against all claims, losses, costs, damages, expenses, action suits and other proceedings, (including reasonable attorney fees), relating to or resulting directly or indirectly from (i) an act or omission of the Vendor, its employees, its agents, or employees of the consortium in the performance of the services provided by this contract, (ii) breach of any of the terms of this RFP or breach of any representation or warranty by the Vendor, (iii) use of the deliverables and or services provided by the Vendor, (iv) infringement of any patent, trademarks, copyrights etc. or such other statutory infringements in respect of all components provided to fulfil the scope of this project.	Vendor shall indemnify, protect and save the Bank and hold the Bank harmless from and against all claims, losses, costs, damages, expenses, action suits and other proceedings, (including reasonable attorney fees), relating to or resulting directly or indirectly from (i) an act or omission of the Vendor, its employees, its agents, or employees of the consortium in the performance of the services provided by this contract, (ii) breach of any of the terms of this RFP or breach of any representation or warranty by the Vendor, (iii) use of the deliverables and or services provided by the Vendor, (iv) infringement of any patent, trademarks, copyrights etc. or such other statutory infringements in respect of all components provided to fulfil the scope of this project.	Clause stands as per RFP.
48	44	5.13 Indemnity	The vendors should indemnify the Bank (including its employees, directors or representatives) from and against claims, losses, and liabilities arising from: · Non-compliance of the vendor with	The vendors should indemnify the Bank (including its employees, directors or representatives) from and against claims, losses, and liabilities arising from: · Non-compliance of the vendor with	Clause stands as per RFP.

			<p>Laws / Governmental Requirements</p> <ul style="list-style-type: none"> · IP infringement · Negligence and misconduct of the Vendor, its employees, and agents · Breach of any terms of RFP, Representation or Warranty · Act or omission in performance of service. 	<p>applicable laws / Governmental Requirements</p> <ul style="list-style-type: none"> · IP infringement · gross Negligence and willful misconduct of the Vendor, its employees, and agents · Breach of any terms of RFP, Representation or Warranty · Act or omission in performance of service. 	
49	45	5.16 Technological Advancements	The Selected bidder shall take reasonable and suitable action, taking into account economic circumstances, at mutually agreed increase /decrease in charges, and the Service Levels, to provide the Services to the Bank at a technological level that will enable the Bank to take advantage of technological advancement in the industry from time to time.	The Selected bidder shall take reasonable and suitable action, taking into account economic circumstances, at mutually agreed increase /decrease in charges, and the Service Levels, to provide the Services to the Bank at a technological level that will enable the Bank to take advantage of technological advancement in the industry from time to time.	Clause stands as per RFP.
50	45	5.17 Guarantee	Selected bidder should guarantee that all the material as deemed suitable for the delivery and management of the Installation, Commission and Maintenance of This MPLS link scope as defined under this document, are licensed and legal. All hardware and software must be supplied with their original and complete printed documentation.	Selected bidder should warrant guarantee that all the material as deemed suitable for the delivery and management of the Installation, Commission and Maintenance of This MPLS link scope as defined under this document, are licensed and legal. All hardware and software must be supplied with their original and complete printed documentation.	Clause stands as per RFP.
51	47	5.19 exit option and contract renegotiation	The Bank will reserve a right to re-negotiate the price and terms of the entire contract with the Selected Bidder at more favourable terms in case such terms are offered in the industry at that time for projects of similar and comparable size, scope and quality.	The Bank will reserve a right to re-negotiate the price and terms of the entire contract with the Selected Bidder at more favourable terms in case such terms are offered in the industry at that time for projects of similar and comparable size, scope and quality.	Clause stands as per RFP.
52	47	5.19 exit option and contract renegotiation	The Bank shall have the sole and absolute discretion to decide whether proper reverse transition mechanism over a period of 6 to 12 months, has been complied with.	The Bank shall have the sole and absolute discretion to decide whether proper reverse transition mechanism over a period of 6 to 12 months, has been complied with.	Clause stands as per RFP.
53	47	5.19 exit option and contract renegotiation	The Bank and the Selected Bidder shall together prepare the Reverse Transition Plan. However, the Bank shall have the sole decision to ascertain whether such Plan has been complied	The Bank and the Selected Bidder shall together prepare the Reverse Transition Plan. Reverse Transition shall be for a period of 2 months and at mutually agreed cost. However, the	Clause stands as per RFP.

			with.	Bank shall have the sole decision to ascertain whether such Plan has been complied with.	
54	49	5.21 Termination	The Bank shall be entitled to terminate the agreement with the Selected bidder at any time by giving ninety (90) days prior written notice to the Selected bidder.	Either party The Bank shall be entitled to terminate the agreement with the Selected bidder at any time by giving ninety (90) days prior written notice to the Selected bidder.	Clause stands as per RFP.
55	49	5.21 Termination	In the event of termination of the Contract due to any cause whatsoever, [whether consequent to the stipulated term of the Contract or otherwise], UCO BANK shall be entitled to impose any such obligations and conditions and issue any clarifications as may be necessary to ensure an efficient transition and effective business continuity of the Service(s) which the selected Vendor shall be obliged to comply with and take all available steps to minimize loss resulting from that termination/breach, and further allow the next successor Vendor to take over the obligations of the erstwhile Vendor in relation to the execution/continued execution of the scope of the Contract.	In the event of termination of the Contract due to any cause whatsoever, [whether consequent to the stipulated term of the Contract or otherwise], UCO BANK shall be entitled to impose any such obligations and conditions and issue any clarifications as may be necessary to ensure an efficient transition and effective business continuity of the Service(s) which the selected Vendor shall be obliged to comply with and take all available steps to minimize loss resulting from that termination/breach, and further allow the next successor Vendor to take over the obligations of the erstwhile Vendor in relation to the execution/continued execution of the scope of the Contract subject to mutually agreed reverse transition plan.	Clause stands as per RFP.
56	50	5.22 Effect of termination	Same terms (including payment terms) which were applicable during the term of the contract/ purchase order should be applicable for reverse transition services.	Same terms (including payment terms) which were applicable during the term of the contract/ purchase order should be applicable for reverse transition services.	Clause stands as per RFP.
57	50	5.22 Effect of termination	The Selected bidder agrees that after completion of the Term or upon earlier termination of the assignment the Selected bidder shall, if required by the Bank, continue to provide maintenance services to the Bank at no less favorable terms than those contained in this scope document. In	The Selected bidder agrees that after completion of the Term or upon earlier termination of the assignment the Selected bidder shall, if required by the Bank, continue to provide maintenance services to the Bank at no less favorable terms than those contained in this scope document.	Clause stands as per RFP.
58	50	5.22 Effect of termination	The Bank shall make such prorated payment for services rendered by the Selected bidder and accepted by the Bank at the sole discretion of the Bank in the event of clause of	The Bank shall make such prorated payment for services rendered by the Selected bidder and accepted by the Bank at the sole discretion of the Bank in the event of clause of	Clause stands as per RFP.

			termination, provided that the Selected bidder is in compliance with its obligations till such date. However, no payment for "costs incurred, or irrevocably committed to, up to the effective date of such termination" will be applicable to Selected Bidder.	termination, provided that the Selected bidder is in compliance with its obligations till such date. However, no payment for "costs incurred, or irrevocably committed to, up to the effective date of such termination" will be applicable to Selected Bidder.	
59	93	Annexure – I Pre-Contract Integrity Pact	3.12 If the BIDDER or any employee of the BIDDER or any person acting on behalf of the BIDDER, either directly or indirectly, is a relative of any of the officers of the BUYER, or alternatively, if any relative of an officer of the BUYER has financial interest/stake in the BIDDER's firm, the same shall be disclosed by the BIDDER at the time of filing of tender.	If the BIDDER or any employee of the BIDDER or any person acting on behalf of the BIDDER, either directly or indirectly, is a relative of any of the officers of the BUYER, or alternatively, if any relative of an officer of the BUYER has financial interest/stake in the BIDDER's firm, the same shall be disclosed by the BIDDER at the time of filing of tender.	Clause stands as per RFP.
60	98	Annexure – I Pre-Contract Integrity Pact 9. Facilitation of Investigation	In case of any allegation of violation of any provisions of this Pact or payment of commission, the BUYER or its agencies shall be entitled to examine all the documents including the Books of Accounts of the BIDDER and the BIDDER shall provide necessary information and documents in English and shall extend all possible help for the purpose of such examination.	In case of any allegation of violation of any provisions of this Pact or payment of commission, the BUYER or its agencies shall be entitled to examine all the documents including the Books of Accounts of the BIDDER and the BIDDER shall provide necessary information and documents in English and shall extend all possible help for the purpose of such examination.	Clause stands as per RFP.
61	96	Annexure – I Pre-Contract Integrity Pact 7. Fall Clause	The BIDDER undertakes that it has not supplied/is not supplying similar product/systems or subsystems at a price lower than that offered in the present bid in respect of any other Ministry/Department of the Government of India or PS U and if it is found at any stage that similar product/systems or sub systems was supplied by the BIDDER to any other Ministry/Department of the Government of India or a PSU at a lower price, then that very price, with due allowance for elapsed time, will be applicable to the present case and the difference in the cost would be refunded by the BIDDER to the BUYER, if the contract has already been concluded.	The BIDDER undertakes that it has not supplied/is not supplying similar product/systems or subsystems at a price lower than that offered in the present bid in respect of any other Ministry/Department of the Government of India or PS U and if it is found at any stage that similar product/systems or sub systems was supplied by the BIDDER to any other Ministry/Department of the Government of India or a PSU at a lower price, then that very price, with due allowance for elapsed time, will be applicable to the present case and the difference in the cost would be refunded by the BIDDER to the BUYER, if the contract has already been concluded.	Please refer corrigendum.
62		New Clause	Upgrades/Updates/Enhancements	Notwithstanding anything to the	Clause stands as per RFP.

				contrary in the RFP, any requirement by the Bank of any upgrade/update/enhancement shall be provided by the Vendor at an additional cost to the Bank and the same shall be done through a Change Order.	
63		New Clause	Savings Clause	Vendor's failure to perform its contractual responsibilities, to perform the services, or to meet agreed service levels shall be excused if and to the extent Vendor's performance is effected , delayed or causes non-performance due to the Bank's omissions or actions whatsoever.	Clause stands as per RFP.
64		New Clause	Deemed Accpetance	Services and/or deliverables shall be deemed to be fully and finally accepted by the Bank in the event when the Bank has not submitted its acceptance or rejection response in writing to Vendor within 15 days from the date of installation/commissioning or when the Bank uses the Deliverable in its business, whichever occurs earlier. Parties agree that Vendor shall have 15 days time to correct in case of any rejection by Client.	
65		New Clause	Site not ready	The Bank hereby agrees to make the site ready as per the agreed specifications, within the agreed timelines. the Bank agrees that Vendor shall not be in any manner be liable for any delay arising out of the Bank's failure to make the site ready within the stipulated period, including but not limited to levy of liquidated damages for any delay in performance of Services under the terms of this Agreement.	Clause stands as per RFP.
66		New Clause	Change Orders	Either party may request a change order ("Change Order") in the event of actual or anticipated change(s) to the agreed scope, Services, Deliverables, schedule, or any other aspect of the Statement of Work. Vendor will prepare a Change Order reflecting the proposed changes, including the impact on the Deliverables, schedule, and fee. In the absence of a signed Change Order, Vendor shall not be	Clause stands as per RFP.

				bound to perform any additional services.	
67		New Clause	Transfer of risk and title	Vendor assumes that the title of ownership and risk of the goods supplied under this Contract is passed onto the Bank on delivery of the material at the the Bank location.	Clause stands as per RFP.
68		New Clause	Pass through warranties	Since Vendor is acting as a reseller of third products, Vendor shall "pass-through" any and all warranties and indemnities received from the manufacturer or licensor of the products and, to the extent, granted by such manufacturer or licensor, the the Bank shall be the beneficiary of such manufacturer's or licensor's warranties and indemnities. Further, it is clarified that Vendor shall not provide any additional warranties and indemnities with respect such products.	Clause stands as per RFP.
69		New Clause	Exceptions to indemnity	Exceptions to Indemnity (a) Vendor shall not have any liability to the Bank under this Section to the extent that any infringement or claim thereof is attributable to: (1) the combination, operation or use of a Deliverable with equipment or software supplied by the Bank where the Deliverable would not itself be infringing; (2) compliance with designs, specifications or instructions provided by the Bank; (3) use of a Deliverable in an application or environment for which it was not designed or contemplated under this Agreement; or (4) modifications of a Deliverable by anyone other than Vendor where the unmodified version of the Deliverable would not have been infringing. Vendor will completely satisfy its obligations hereunder if, after receiving notice of a claim, Vendor obtains for the Bank the right to continue using such Deliverables as provided without infringement, or replace or modify such Deliverables so that they become non-infringing.	Clause stands as per RFP.
70		New Clause	Termination of Contract	Either Party shall have the right to terminate this Agreement at any time: With Cause – in the event that the	Clause stands as per RFP.

				<p>other party commits a material breach of the Agreement and fails to cure such default to the non-defaulting party's reasonable satisfaction within thirty (30) days.</p> <p>In the event of termination by Bank, the bidder/Vendor shall be paid for the:</p> <ol style="list-style-type: none"> 1. goods delivered 2. services rendered 3. work in progress 4. unpaid AMCs 5. third party orders in pipeline which cannot be cancelled despite bidder/vendor's best efforts 6. unrecovered investments shall be paid by the Bank as per termination schedule till the date of termination. 	
71	68	Required Minimum Technical Features of Firewall	Firewall performance should be minimum 20 Gbps (realworld throughput)	Performance asked should be clearly specified that Total real world throughput must be 20 Gbps after enabling IPS, Anti-malware, URL Filtering, application Control, Anti-Bot, Sandboxing, QoS and NOT JUST FIREWALL . The Specifications mentioned is clear that the device must have all the above features. If we need to consider only Firewall performance, the device sizing will drastically change. Please Clarify.	Please refer modified technical requirement of firewall in corrigendum.
72	73	Required Minimum Technical Features of Firewall	The solution must provide a full - featured NBA capability to detect threats emerging from inside the network This includes analysis techniques (e.g., NetFlow) and the ability to detect deviations from normal baselines	OEM Specific. Please remove	Please refer modified technical requirement of firewall in corrigendum.
73	74	Required Minimum Technical Features of Firewall	The NBA capability must provide visibility into how network bandwidth is consumed to aid in troubleshooting network outages and performance degradations.	OEM Specific. Please remove	Please refer modified technical requirement of firewall in corrigendum.
74	74	Required Minimum Technical Features of Firewall	The NBA capability must provide the ability to link Active Directory and/or LDAP usernames to IP addresses related to suspected security events.	OEM Specific. Please remove	Please refer modified technical requirement of firewall in corrigendum.
75	74	Required Minimum Technical Features of Firewall	The same network devices used for IPS must also be used as part of the NBA capability. No NBA -only device should	OEM Specific. Please remove	Please refer modified technical requirement of firewall in corrigendum.

			be required.		
76	74	Required Minimum Technical Features of Firewall	The same management platform used for IPS must also be used to manage the NBA capability. No NBA-only management components should be required.	OEM Specific. Please remove	Please refer modified technical requirement of firewall in corrigendum.
77	74	Required Minimum Technical Features of Firewall	The management platform must be accessible via a web-based interface and ideally with no need for additional client software.	This is not secure and specific to few OEMs. Please remove	Please refer modified technical requirement of firewall in corrigendum.
78	70	Required Minimum Technical Features of Firewall	Solution should provide high Threat protection rate minimum of 99%.	Please clarify how this needs to be validated?	Please refer modified technical requirement of firewall in corrigendum.
79	76	Required Minimum Technical Features of Firewall	The proposed device should have Intrusion prevention sensors delivering a minimum of 10 Gbps of context-aware , real-world traffic inspection	Please clarify whether this throughput performance is considering bi-directional scanning and customized profiling	Please refer modified technical requirement of firewall in corrigendum.
80		Annexure G – Sl. No. 3	The solution should be a on premise Secure Web Gateway solution having Proxy, user based URL filter, user based Application filtering on mobile devices like blocking of WhatsApp, Caching, SSL Inspection, Anti-Virus, Antimalware, spyware blocking, blocking of Peer-Peer applications like Kazaa, Gnutella, Bit Torrent, IRC (over HTTP) , including blocking of voice and video services and real-time protection against zero day threats all in one solution(Appliance or software installed in Server).	Blocking of Voice is not possible as it over UDP and proxy supports only TCP. The solution should be a on premise Secure Web Gateway solution having Proxy, user based URL filter, user based Application filtering on mobile devices like blocking of WhatsApp, Caching, SSL Inspection, Anti-Virus, Antimalware, spyware blocking, blocking of Peer-Peer applications like Kazaa, Gnutella, Bit Torrent, IRC (over HTTP) , including blocking of video services and real-time protection against zero day threats all in one solution(Appliance or software installed in Server).	Please refer modified technical requirement of proxy in corrigendum.
81		Annexure G – sl. No. 5	The solution will be deployed on physical servers (not Virtual systems) / appliance and should be manageable through single unified management console. Solution should support Real-Time Session tracking.	Real time session tracking do not support any proxy solution. The solution will be deployed on physical servers (not Virtual systems) / appliance and should be manageable through single unified management console. Solution should support Real-Time Security Scanning.	Please refer modified technical requirement of proxy in corrigendum.
82		Annexure G – sl. no. 14	The solution should be possible to limit bandwidth usage for specific categories, applications and protocols	Bandwidth limit and application can not be controlled by any proxy solutions. Bandwidth can be optimize and it can block after reaching it's optimization level. The solution should be possible to optimize bandwidth usage for specific categories and protocols.	Please refer modified technical requirement of proxy in corrigendum.
83		Annexure G – sl. no. 21	The solution should support all network communication/application protocols	SMTP,587 and SPOP3 is for the Email. Proxy checks for only HTTP,	Please refer modified technical requirement of proxy in

			& ports like http,https,SMTP,587,SPOP3,443 etc.	HTTPS,FTP,SFTP. The solution should support all network communication/application protocols & ports like HTTP, 443 HTTPS,FTP,SFTP etc	corrigendum.
84		Annexure G – sl. no. 33	The solution must support, control and recognize al Web application traffic and protect against Web based attacks.	Proxy works on http and https only. Web based attacks should be based on http or https. The solution must support, control and recognize al Web application traffic and protect against Web based attacks over HTTP and HTTPS.	Please refer modified technical requirement of proxy in corrigendum.
85		Annexure G – sl. no. 87	System should generate Reports Identifying Users by AD Name, IP, or Mac Address	Mac address can be fetched only through the endpoint agents. As Web Security placed at Gateway and there are no agents needed so Mac address cannot be fetched by any proxy solutions. System should generate Reports Identifying Users by AD Name or IP based.	Please refer modified technical requirement of proxy in corrigendum.
86		Annexure G – sl. no. 88	Proposed system should have at least 3 no. of 100/1000 interfaces Ethernet Interface RJ45 and have WAN Load balance function.	WAN load balance is of Link load balancer. not proxy. Proposed system should have at least 3 no. of 100/1000 interfaces Ethernet Interface RJ45.	Please refer modified technical requirement of proxy in corrigendum.
87		General		Should HA be considered for proposed solution?	NO
88		Annexure - K	License Cost for 500 Users (Qty 7)	Does it mean that within 3 years the additional license if required will be purchased in set of 500 users?	Yes
89				It is mentioned that the proposed Solution should have support for 5 years, however price is asked for only 3 years. So the price for 4th and 5th year will again be considered at the end of 3 rd year.	Please refer warranty point in corrigendum.
90	18	2.1 Eligibility criteria	4. The Bidder should have involved in Supply, Installation, Configuration & Maintenance of Network devices (Software and Hardware), management & monitoring of MPLS/P2P and ISDN links and providing related services for at least 5 years in 2 nos. of Govt. Financial Institution/Bank in India having minimum 2500 branches/office network in each organization, out of which one should be Public Sector Bank.	Kindly Clarify whether, "the 2500 Branches/Offices are related to "Supply, Installation, Configuration & Maintenance of Network devices (Software and Hardware), management & monitoring of MPLS/P2P and ISDN links and providing related services" OR "Govt. Financial Institution/Bank in India"	Clause stands as per RFP
91	18	2.1 Eligibility criteria	4. The Bidder should have involved in Supply, Installation, Configuration &	Request to consider All BSFI Institution s instead of Only Govt. Financial	Clause stands as per RFP

			Maintenance of Network devices (Software and Hardware), management & monitoring of MPLS/P2P and ISDN links and providing related services for at least 5 years in 2 nos. of Govt. Financial Institution/Bank in India having minimum 2500 branches/office network in each organization, out of which one should be Public Sector Bank	Institution/banks as the technological experience will be same across all financial Organizations. Hence Request to modify the clause as: The Bidder should have involved in Supply, Installation, Configuration & Maintenance of Network devices (Software and Hardware), management & monitoring of MPLS/P2P / ISDN links and providing related services for at least 3 years in 2 nos. of Govt. Financial Institution/BSFI in India having minimum 2500 branches/office network in each organization, out of which one should be Public Sector Bank	
92	18	2.1 Eligibility criteria	The Proposed OEM's network equipment for branches (Router & Switch) should be running in 1500 branches in a Public Sector Bank at time of submission of this RFP.---- Purchase order in name of bidder and execution certificate from existing customer(s).	Experience shall not be less with projects executed of other OEMs with either of networking equipments (Router & Switches) across all critical mission BSFI entities. Hence Request you to Modify the clause as: The network equipment for branches (Router / Switch) should be running in 1500 branches in a Public Sector Bank/BSFI at time of submission of this RFP.---- Purchase order in name of bidder and execution certificate from existing customer(s).	Clause stands as per RFP.
93	18	2.1 Eligibility criteria	The Proposed OEM's network equipment for branches (Router & Switch) should be running in 1500 branches in a Public Sector Bank at time of submission of this RFP.---- Purchase order in name of bidder and execution certificate from existing customer(s).	Experience shall not be less with projects executed of other OEMs with either of networking equipments (Router & Switches) across all critical mission BSFI entities. Hence Request you to Modify the clause as: The network equipment (all types) for datacenter should be running in a PSU Bank/BSFI having minimum 2500 branches at time of submission of this RFP	Clause stands as per RFP
94	37	5.3 Installation and commissioning	Bidder has to commission the links at DC and DR within 4 weeks and all other links within 6 weeks	With the Complexity and Size of the Project request you to extend the delivery time line to 6-8 weeks instead of 4 weeks	Clause stands as per RFP
95	23	4.1 Summary of the Requirement	iv) Support services for routers, switch, and security devices at the core distribution and access WAN locations.-	Do we need to provide OEM warranty support as well, as part of support services, or UCO Bank will cover all the relevant HW in the scope for requisite OEM warranties?	Bidder must have back to back support relation with the OEM's whose products are followed by the bidder to the Bank, in case the bidder is not Original Equipment Manufacturer(OEM). A commitment

					letter (Annexure C) from the OEM(s) has to be submitted along with the Technical bid in this regard at least for a period of 5 years for all new and support upto end of life for all product under AMC as per Annexure J & M.
96	23	4.1 Summary of the Requirement	viii) AMC of network equipment at DC, DR site, Head Offices, Zonal Offices, Branches as per Annexure -L - kindly clarify how this scope is different from point iv above	Kindly clarify how this scope is different from point iv above.	Clause read as: AMC of network equipment at DC, DR site, Head Offices, Zonal Offices, Branches as per <u>Annexure -M & J</u>
97	24	4.3 On site Manpower Assignment	iii) Manpower	We assume that total headcounts for these 43 seats would be min 53 nos. owing to few seats are 24X7. Kindly confirm	Clause stands as per RFP
98	24	4.4 WAN network monitoring	III) Monitoring of all the network devices-	We assume all devices here means only WAN devices as per annexure-L, and does not include LAN network of the locations. Please confirm	All network device & LAN at DC & DR site and branch up to network switch.
99		General		we assume that all the management functionalities asked in the SOW e.g. performance management, change management, asset management, monitoring, helpdesk, availability reporting etc. are either supported in the current NMS software or bank will provide additional tools if required. Scope of the vendor is only limited to performing the tasks, not the supply of the tools. Kindly confirm.	Bank will only provide NMS software for link monitoring. To Comply all points in SOW is bidder responsibility.
100	36	4.67	The bidder has to ensure that any equipment to be supplied as part of this RFP should not have either reached end of sales for at least 3 years post-date of acceptance of such equipment by the Bank- no bidder or OEM can ensure that product does not to end of sale after 3 yrs of installation (which is roughly at least 3.5 yrs after bid submission). Kindly remove this clause. The bidder can however ensure that the product will not be end of sale at the time of bidding, and does not go end of support during the contract period of 3 yrs + 2 yrs.	No bidder or OEM can ensure that product does not to end of sale after 3 yrs of installation (which is roughly at least 3.5 yrs after bid submission). Kindly remove this clause. The bidder can however ensure that the product will not be end of sale at the time of bidding, and does not go end of support during the contract period of 3 yrs + 2 yrs.	Clause stands as per RFP.
101	37	5.3.1	Deliveries of the new networks equipment/device/solution, installation and operationalization of complete	Kindly change this to minimum 10 weeks from firm purchase order, since OEM supplies itself will take min 6-8	Clause stands as per RFP.

			solution at all locations should be made within 4 weeks from the date of purchase order - kindly change this to minimum 10 weeks from firm purchase order, since OEM supplies itself will take min 6-8 weeks.	weeks.	
102		SLA & Penalties general query-		SLA and penalties are very stringent. Request revision of the same. Also, it is assumed that all the link service providers/ equipment vendors are bound to the asked or higher SLAs to allow the bidder to successfully honor the said SLAs.	Clause stands as per RFP.
103	44			Example of SLA computation does not seem to be correct since it is subtracting scheduled downtime as well. Kindly suggest.	Please refer corrigendum.
104	60	Annexure – G	Product specifications- general query- Product must not be End of Life and Support for next 3 years/ 5 years- kindly suggest which of the 2 periods- 3 years or 5 years, is correct.	Kindly suggest which of the 2 periods- 3 years or 5 years, is correct.	Please refer corrigendum warranty point.
105		Annexure – A & F	general query- Table A mentions new products to be offered, and table F provides details of the replacement products	Kindly suggest if the table A's products are also covered in tale F or are altogether new requirement.	Table A in Annexure J for network devices of new branches. Table F in Annexure J for old existing product replacement.
106		Annexure – K	General query	It seems that all the services asked in the SOW are not covered in this commercial template (e.g. FMS services, manpower cost etc.). Kindly suggest and modify the commercial sheet as appropriate.	Table D in Annexure J & K for Network Link Management Service including FM & Man Power service.
107			General query	We assume that the details given after Annexure K till page 214 form annexure L, and from page 215 to the end form Annexure-M. Kindly confirm. Kindly also provide softcopy of these details to allow the bidders quick analysis of support services requisites.	ANNEXURE - L109 ANNEXURE - M.....215
108		Additional Spec for Modem	We request you to include the driving distance of G.703(at exchange) & V.35(at branch)modems on SHDSL port as 6.5KM in spec., as it is completely missing	Better distance offered with 6.5km	Please refer modified technical requirement of modem in corrigendum
109	page 88	Modem management	(1)SHDSL Operating Range in KM on 0.5mm cable: 2 wire: 6.5 Km @ 2Mbps, 7.4 Km @ 1 Mbps, 10.5 Km @ 64 Kbps (2) Point No.8 in page No. 82 to be modified as " Management Via	Justification: Now a days no manufacturer is providing RS-232 terminal port for console access in either Desktops or Laptops , hence we recommend you to mention	Please refer modified technical requirement of modem in corrigendum

			„10/100BaseT out of Band Management"	Management Via Ethernet only. Dial in and Dial out is not applicable for modem management.	
110	11	1.2.24	A commitment letter from the OEM has to be submitted along with the Technical bid in this regard at least for a period of 5 years.	The Total contract is for 3 years . However, the commitment being asked is for 5 years . Request you to confirm	Please refer corrigendum warranty clause.
111	11	1.2.25	The bidder shall not quote for the products, whose End of sale/ End of Support / End of Life has been declared by the OEM. The Bidder has to ensure that any equipment supplied as part of this RFP should not reach end of support or end of life for at least 5 years postdate of acceptance of such equipment by the Bank.	Some of the equipments will be refreshed in Y2/Y3 of the contract & no OEM will give commitment for those equipments for end of support/life post 5 years post acceptance. Request you to make the necessary change accordingly.	Please refer corrigendum warranty clause.
112	21	Part IV Scope of Work	Other Details M/s BSNL is primary MPLS, ISDN & CDMA service provider. Backhaul link for BSNL MPLS link & CDMA connectivity should be managed by bidder.	Please confirm whether the bidder needs to manage only the Backhaul link not the primary link.	M/s BSNL is primary MPLS, ISDN & CDMA service provider. Backhaul link for BSNL MPLS link & CDMA connectivity should also be managed by bidder.
113	29	4.16 Inventory Management	iii) Quarterly submission of all network devices inventory (Branches and hub locations) report, on site visit and signed by the branch Location head.	Please clarify, Inventory management should be done centrally and signed centrally at Datacenter.	Yes
114	30	4.18 Helpdesk	ISDN utilization report with detail event and clarification. Extra usage will be deducted from vendor in case of SLA mismatch for that link.	Please elaborate the requirement	Any misused of ISDN bill will be deducted from vendor payment.
115	36	4.67	The bidder has to ensure that any equipment to be supplied as part of this RFP should not have either reached end of sales for at least 3 years post-date of acceptance of such equipment by the Bank.	Request you to modify the clause as "The bidder has to ensure that any equipment to be supplied as part of this RFP should not have either reached end of sales/declared end of sale at the time of signing the contract to the Bank.	Clause stands as per RFP.
116	36	4.67	Further any equipment supplied by the bidder, should not have reached end of support/life for at least 2 years from the date of contract expiry.	All OEMs gives commitment of end of Support for 5 years from the declaration of end of sale . Request you to delete the clause	Clause stands as per RFP.
117	37	5.3.1	Installation and commissioning Deliveries of the new networks equipment/device/solution, installation and operationalization of complete solution at all locations should be made within 4 weeks from the date of purchase order.	For the Equipments that will be refreshed in Y1 at the start of contract , request you to modify the clause as " Deliveries of the new networks equipment/device & installation at all locations should be made within 10 weeks from the date of purchase order"	Clause stands as per RFP.
118	38	5.5	The cost of network link must include rental charges of network equipment's	Please elaborate the requirement	Please refer corrigendum Price clause.

			e.g modem, repeater, etc. required to be terminated the link at CPE Ethernet interface. The Price Bid also must include all applicable taxes such as Sales/Service/VAT / Waybill etc. The Octroi /Entry Tax will be paid extra, wherever applicable on submission of actual Tax receipt.		
119	27	4.9 Maintenance of existing Networking Equipment	Successful Bidder has to maintain the equipments supplied by him and the equipments under AMC with him and keep sufficient spare parts for maintaining the uptime of the equipment/site	Can we replace the Faulty Equipment with equivalent spec of different OEM	In case of damage of any equipment under AMC, bidder should replace with same equipment. In case same replacement equipment not available in market or out of sell by OEM, then bidder should replace with equivalent/higher product.
120	60	Annexure G, Router- Type A	Chassis based & modular architecture for scalability and should be a single box configuration for ease of management.	We understand the requirement of the RFP is to have Branch Routers. Chassis Based generally points towards Core Routers. Request to modify clause as "Modular architecture for scalability and should be a single box configuration for ease of management."	Please refer modified technical requirement of router in corrigendum
121	60	Annexure G, Router- Type A	Support for the following IP v6 features : RIP NG , OSPF v3 , BGP Support for V6, IP V6 Dual Stack, NAT 64, IP v6 Policy based Routing, and IP v6 QoS, SNMP V3 over IPv6	We understand the requirement here is to achieve seamless IPv6 transition from IPv4 for UCOBANK. There are a number of transition mechanisms are available and different OEMs adopt different mechanisms to address this requirement. Request pls generalize the clause which will bring wider competition. Request to modify the clause as below " Support for the following IP v6 features : RIP NG , OSPF v3 , BGP Support for V6, IP V6 Dual Stack, NAT 64/Suitable Network address translation/tunneling for IPv6, IP v6 Policy based Routing, and IP v6 QoS, SNMP V3 over IPv6"	Please refer modified technical requirement of router in corrigendum
122	61	Annexure G, Router- Type A	The router should support IPSec Framework for Secured Data transfer Key Exchange : Internet Key Exchange (IKE), IKEv2, Pre-Shared Keys (PSK), Public Key Infrastructure PKI (X.509), RSA encrypted nonces etc, IPSec Data Encapsulation AH and ESP	As the best practice Two authentication methods are used to authenticate between 2 Peers : pre-shared key authentication and PKI-based digital signature authentication (RSA Signature).Request to modify the clause as below" The router should support IPSec Framework for Secured Data transfer Key Exchange : Internet Key Exchange (IKE), IKEv2,	Please refer modified technical requirement of router in corrigendum

				Pre-Shared Keys (PSK), Public Key Infrastructure PKI (X.509), RSA encrypted nonces/ RSA Signatures etc, IPSec Data Encapsulation AH and ESP".	
123	62	Annexure- G Router- Type B	Chassis based & modular architecture for scalability and should be a single box configuration for ease of management.	We understand the requirement of the RFP is to have Branch Routers. Chassis Based generally points towards Core Routers. Request to modify clause as "Modular architecture for scalability and should be a single box configuration for ease of management."	Please refer modified technical requirement of router in corrigendum
124	62	Annexure- G Router- Type B	The router should support IPSec Framework for Secured Data transfer Key Exchange : Internet Key Exchange (IKE), IKEv2, Pre-Shared Keys (PSK), Public Key Infrastructure PKI (X.509), RSA encrypted nonces etc, IPSec Data Encapsulation AH and ESP	As the best practice Two authentication methods are used to authenticate between 2 Peers : pre-shared key authentication and PKI-based digital signature authentication (RSA Signature).Request to modify the clause as below" The router should support IPSec Framework for Secured Data transfer Key Exchange : Internet Key Exchange (IKE), IKEv2, Pre-Shared Keys (PSK), Public Key Infrastructure PKI (X.509), RSA encrypted nonces/ RSA Signatures etc, IPSec Data Encapsulation AH and ESP".	Please refer modified technical requirement of router in corrigendum
125	63	Annexure- G Router- Type C	Chassis based & modular architecture for scalability and should be a single box configuration for ease of management.	We understand the requirement of the RFP is to have Branch Routers. Chassis Based generally points towards Core Routers. Request to modify clause as "Modular architecture for scalability and should be a single box configuration for ease of management."	Please refer modified technical requirement of router in corrigendum
126	64	Annexure- G Router- Type C	Support for the following IP v6 features : RIP NG , OSPF v3 , BGP Support for V6, IP V6 Dual Stack, NAT 64, IP v6 Policy based Routing, and IP v6 QoS, SNMP V3 over IPv6	We understand the requirement here is to achieve seamless IPv6 transition from IPv4 for UCOBANK. There are a number of transition mechanisms are available and different OEMs adopt different mechanisms to address this requirement. Request pls generalize the clause which will bring wider competition. Request to modify the clause as below " Support for the following IP v6 features : RIP NG , OSPF v3 , BGP Support for V6, IP V6 Dual Stack, NAT 64/Suitable Network address translation/tunneling for IPv6, IP v6 Policy based Routing, and IP v6 QoS, SNMP V3 over IPv6"	Please refer modified technical requirement of router in corrigendum
127	65	Annexure- G Router- Type C	The router should support IPSec Framework for Secured Data transfer	As the best practice Two authentication methods	Please refer modified technical requirement of router in

			Key Exchange : Internet Key Exchange (IKE), IKEv2, Pre-Shared Keys (PSK), Public Key Infrastructure PKI (X.509), RSA encrypted nonces etc, IPsec Data Encapsulation AH and ESP	are used to authenticate between 2 Peers : pre-shared key authentication and PKI-based digital signature authentication (RSA Signature).Request to modify the clause as below" The router should support IPsec Framework for Secured Data transfer Key Exchange : Internet Key Exchange (IKE), IKEv2, Pre-Shared Keys (PSK), Public Key Infrastructure PKI (X.509), RSA encrypted nonces/ RSA Signatures etc, IPsec Data Encapsulation AH and ESP".	corrigendum
128	65	Annexure G, Switch - Type A	Chassis based & modular architecture for scalability and should be a single box configuration for ease of management	We understand the requirement of the RFP is to have Fixed Configuration Switches . Chassis Based generally points towards High End Switches. Request to modify clause as " Modular architecture for scalability and should be a single box configuration for ease of management."	Please refer modified technical requirement of switch in corrigendum
129	66	Annexure G, Switch - Type A	Should support NAT, PAT, DHCP	NAT& PAT are firewall features and not a relevant features in Switches. Also separate Firewall have been asked. Please remove NAT & PAT	Please refer modified technical requirement of switch in corrigendum
130	66	Annexure G, Switch - Type B	Chassis based & modular architecture for scalability and should be a single box configuration for ease of management.	We understand the requirement of the RFP is to have Fixed Configuration Switches . Chassis Based generally points towards High End Switches. Request to modify clause as " Modular architecture for scalability and should be a single box configuration for ease of management."	Please refer modified technical requirement of switch in corrigendum
131	68	Required minimum technical Specification for Firewall	Chassis based & modular architecture for scalability	Different OEM have different architecture. Some use modular & chasis based architecture to support more number of interfaces in future with extra cost involved & some provides more number of interfaces from day one as an integrated option on the same appliance without any extra cost. So requesting to make this point as optional.	Please refer modified technical requirement of firewall in corrigendum
132	68	Required minimum technical Specification for Firewall	Should have a 64Bit Multi-Core Processor and should not be ASIC based architecture	Different OEM have different architecture. Some works on Multicore Processor based architecture & some works on ASIC architecture. More over ASIC architcture provides much more stable performance than Multicore because of its Multiple CPU processing structure compared to single CPU	Please refer modified technical requirement of firewall in corrigendum

				processing where all the functionalities are handled by a single processor only & performance degrades as on when all the security functionalities are enabled. So kindly relax this point as "Multicore or ASIC based architecture" to make the spec generic	
133	68	Required minimum technical Specification for Firewall	Support for minimum 1000 MAC addresses	This high value capacity of MAC address support is favouring to one particular OEM. Kindly relax this 200 so that all reputed OEM can comply with competitive models	Please refer modified technical requirement of firewall in corrigendum
134	70	Required minimum technical Specification for Firewall	The solution should have capability to fully reveal malware's current and potential payloads.	It's biased to specific OEM. Cloud Sandboxing solution integrated with Firewall helps detect & prevent from Advanced Persistent Threats or Zero day attacks. But this much detailed reporting functionality on those detected malwares is available with dedicated Sandbox appliances. As this is a requirement of a Firewall so the main concern should be the detection & prevention of the malwares. So requesting to remove this point or make it optional.	Please refer modified technical requirement of firewall in corrigendum
135	70	Required minimum technical Specification for Firewall	The solution should provide a detailed list of every DLL and API referenced, all header information about the binary, and complete assembly-language listing of the binary code.	It's biased to specific OEM. Cloud Sandboxing solution integrated with Firewall helps detect & prevent from Advanced Persistent Threats or Zero day attacks. But this much detailed reporting functionality on those detected malwares is available with dedicated Sandbox appliances. As this is a requirement of a Firewall so the main concern should be the detection & prevention of the malwares. So requesting to remove this point or make it optional.	Please refer modified technical requirement of firewall in corrigendum
136	70	Required minimum technical Specification for Firewall	The solution should provide reports to shows all the activities the malware code performs related to file systems, Windows registry, network operations, Processes and any other miscellaneous operations	It's biased to specific OEM. Cloud Sandboxing solution integrated with Firewall helps detect & prevent from Advanced Persistent Threats or Zero day attacks. But this much detailed reporting functionality on those detected malwares is available with dedicated Sandbox appliances. As this is a requirement of a Firewall so the main concern should be the detection & prevention of the malwares. So requesting to remove this point or make	Please refer modified technical requirement of firewall in corrigendum

				it optional.	
137	70	Required minimum technical Specification for Firewall	The solution should provide summary for instance, whether the malware wrote into a certain file, modified a registry setting, opened a port or communicated to a specific url, or changed the name of a running process to hide itself.	It's biased to specific OEM. Cloud Sandboxing solution integrated with Firewall helps detect & prevent from Advanced Persistent Threats or Zero day attacks. But this much detailed reporting functionality on those detected malwares is available with dedicated Sandbox appliances. As this is a requirement of a Firewall so the main concern should be the detection & prevention of the malwares. So requesting to remove this point or make it optional.	Please refer modified technical requirement of firewall in corrigendum
138	70	Required minimum technical Specification for Firewall	Solution should provide Detailed Technical Report, Behavior Summary Report and a Logic Execution Path Map.	It's biased to specific OEM. Cloud Sandboxing solution integrated with Firewall helps detect & prevent from Advanced Persistent Threats or Zero day attacks. But this much detailed reporting functionality on those detected malwares is available with dedicated Sandbox appliances. As this is a requirement of a Firewall so the main concern should be the detection & prevention of the malwares. So requesting to remove this point or make it optional.	Please refer modified technical requirement of firewall in corrigendum
139	70	Required minimum technical Specification for Firewall	The solution must be capable of significantly reducing operator effort and accelerating response to threats by automatically prioritizing alerts, ideally based on the potential for correlated threats to successfully impact the specific hosts they are directed toward.	Kindly remove this as it's biased to specific OEM	Please refer modified technical requirement of firewall in corrigendum
140	72	Required minimum technical Specification for Firewall	Solution must be capable of passively gathering information about network hosts and their activities, such as operating system, services, open ports, client applications, and vulnerabilities, to assist with multiple activities, such as intrusion event data correlation, elimination of false positives, and policy compliance.	It's a dedicated feature of a specific OEM. So requesting to remove this point .	Please refer modified technical requirement of firewall in corrigendum
141	73	Required minimum technical Specification for Firewall	The solution must be capable of significantly reducing operator effort and accelerating response to threats by automatically prioritizing alerts, ideally based on the	Kindly remove this as it's biased to specific OEM	Please refer modified technical requirement of firewall in corrigendum

			potential for correlated threats to successfully impact the specific hosts they are directed toward.		
142	73	Required minimum technical Specification for Firewall	The solution must be capable of dynamically tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.) with minimal human intervention.	Kindly remove this as it's biased to specific OEM	Please refer modified technical requirement of firewall in corrigendum
143	73	Required minimum technical Specification for Firewall	The solution must provide a full-featured NBA capability to detect threats emerging from inside the network This includes the ability to establish "normal" traffic baselines through flow analysis techniques (e.g., NetFlow) and the ability to detect deviations from normal baselines	It's a fully biased point of OEM. None of the other reputed OEMs who are there in Gartner leaders or challengers have their own NBA. So requesting to remove this point	Please refer modified technical requirement of firewall in corrigendum
144		Required minimum technical Specification for Firewall	The management platform must include flexible workflow capabilities for managing the complete life cycle of an event, from initial notification through to any response and resolution activities that might be required.	Kindly remove this as it's biased to specific OEM	Please refer modified technical requirement of firewall in corrigendum
145	76	Required Minimum Technical Features of IPS	(General)	Procuring state of the art security solutions is vert critical for all large organizations like yours. Hence we would propose you to choose among the Gartner Leader for your IPS requirement. Please add a clause stating "Proposed IPS solution should be from the leaders quadrant of the latest gartner report". There are 3 vendors in this quadrant hence you would be able to procure best of the breed solution without compromising on the total cost of the project.	Please refer modified technical requirement of IPS in corrigendum
146	76	Required Minimum Technical Features of IPS/ Point 15	The IPS should be able to inspect SSL/https traffic	We have send some deployments where-in the OEM has proposed a separate applaince/module to do this SSL inspection. This has caused latency and are not able to meet the clause 19 "The average latency of the proposed IPS should be less than 150 microseconds". Hence we propose that you modify this clause to "The IPS should be able to inspect SSL/https traffic. SSL inspection should be a built-in feature of the same applaince"	Please refer modified technical requirement of IPS in corrigendum
147	76	Required Minimum Technical Features of IPS / Point 1	IPS should The appliance should be rack mountable and support side rails if required	We recommend that the IPS should be a dedicated applaince rather than part of a UTM. Hence we request you	Please refer modified technical requirement of IPS in corrigendum

				to please modify the spec to "IPS appliance should purpose built and not part of an integrated solution. It should be rack mountable and support side rails if required"	
148	77	Required Minimum Technical Features of IPS / Point 28	Proposed IPS solution should support Vulnerability and Exploit signatures, Protocol validation, Anomaly detection, Behaviour based detection, Multi-element global correlation and reputation based filtering	The part "Multi-element global correlation" is limited to single OEM. Hence we would remove that part of the spec and change it to "Proposed IPS solution should support Vulnerability and Exploit signatures, Protocol validation, Anomaly detection, Behaviour based detection, correlation and reputation based filtering". Every vendor have their own way to doing correlation based filtering.	Please refer modified technical requirement of IPS in corrigendum
149	80	Annexure G	The solution must support acceleration for Server Message Block Version 2 (SMBv2) and signed SMBv2 protocols.	Do you also require optimization for SMB v3 which is available on latest MS Windows Server and Client OS?	Please refer modified technical requirement of WAN Optimizer in corrigendum
150	78	Annexure G	Should support optimization for minimum of 10,000 concurrent TCP connections from day one, with scalability option when configured in full transparency mode	10000 concurrent connection are very less for 1000 mbps unit. It should be 100000 concurrent connections. Please clarify if this is typographical error or	Please refer modified technical requirement of WAN Optimizer in corrigendum
151	78	Annexure G	Primary Data Center, Bangalore and Disaster Recovery Site, Kolkata. The WAN Optimization solution is being procured for 4 international Branches.	Do you required HA solution for DC and DR	Yes HA at DC & DR site
152	78	Annexure G	Primary Data Center, Bangalore and Disaster Recovery Site, Kolkata. The WAN Optimization solution is being procured for 4 international Branches.	Which replication applications (SRDF/A, Snapmirror, Oracle Data Guard etc.) are being between DC and DR	Oracle Data Guard.
153	78	Annexure G	Primary Data Center, Bangalore and Disaster Recovery Site, Kolkata. The WAN Optimization solution is being procured for 4 international Branches.	Do you use any FCIP switch/router for replication? If Yes, please provide make and model details	Router
154	78	Annexure G	Primary Data Center, Bangalore and Disaster Recovery Site, Kolkata. The WAN Optimization solution is being procured for 4 international Branches.	Do you use any FCIP switch/router for replication? If Yes, please provide make and model details	Router
155	78	Annexure G	Primary Data Center, Bangalore and Disaster Recovery Site, Kolkata. The WAN Optimization solution is being procured for 4	What is the WAN Bandwidth at Bangalore DC and Kolkata DR sites	84 Mbps

			international Branches.		
156	81	Annexure G	Branch Wan Optimizer: Branch solution should have WAN optimization functionality from day one through external appliance for supporting minimum of 150 Concurrent TCP Connections for each of 4 No of International Branches with concurrent users upto 30 per branch. For 4 branches with concurrent users more than 20 per branch , WAN optimization should support minimum of 120 TCP connections. WAN Optimization solution should have the capability to seamlessly integrate & optimize IPsec VPN interested traffic along with application acceleration supporting applications i.e. Finacle, ATM, Mail Messaging (Exchange 2010), WEB Portal,etc. originating from Branch/office locations. The WAN Optimization solution is being procured for 4 international Branches.	Do you require solution for 4 branches with 30 and 4 branches with 20 users separately or only for 4 branches?	Please refer modified technical requirement of WAN Optimizer in corrigendum
157	81	Annexure G	Branch Wan Optimizer: Branch solution should have WAN optimization functionality from day one through external appliance for supporting minimum of 150 Concurrent TCP Connections for each of 4 No of International Branches with concurrent users upto 30 per branch. For 4 branches with concurrent users more than 20 per branch , WAN optimization should support minimum of 120 TCP connections. WAN Optimization solution should have the capability to seamlessly integrate & optimize IPsec VPN interested traffic along with application acceleration supporting applications i.e. Finacle, ATM, Mail Messaging (Exchange 2010), WEB Portal,etc. originating from Branch/office	What is WAN Bandwidth at Branch sites	64/128/256/512/2048/4096/8192 Kbps

			locations. The WAN Optimization solution is being procured for 4 international Branches.		
158	81	Annexure G	Branch Wan Optimizer: Branch solution should have WAN optimization functionality from day one through external appliance for supporting minimum of 150 Concurrent TCP Connections for each of 4 No of International Branches with concurrent users upto 30 per branch. For 4 branches with concurrent users more than 20 per branch , WAN optimization should support minimum of 120 TCP connections. WAN Optimization solution should have the capability to seamlessly integrate & optimize IPsec VPN interested traffic along with application acceleration supporting applications i.e. Finacle, ATM, Mail Messaging (Exchange 2010), WEB Portal,etc. originating from Branch/office locations. The WAN Optimization solution is being procured for 4 international Branches.	Do you need Infosys certified solution for Finacle Optimization?	No
159	81	Annexure G	"Branch Wan Optimizer: Branch solution should have WAN optimization functionality from day one through external appliance for supporting minimum of 150 Concurrent TCP Connections for each of 4 No of International Branches with concurrent users upto 30 per branch. For 4 branches with concurrent users more than 20 per branch , WAN optimization should support minimum of 120 TCP connections. WAN Optimization solution should have the capability to seamlessly integrate & optimize IPsec VPN interested traffic along with application acceleration supporting applications i.e. Finacle, ATM, Mail Messaging (Exchange 2010),	Which Finacle version is in use?	Finacle version 7.X for Domestic. Finacle version 10.X for International.

			WEB Portal,etc. originating from Branch/office locations. The WAN Optimization solution is being procured for 4 international Branches." Do you need Infosys certified solution for Finacle Optimization?		
160	7 9 16 58 59	Part 1 - Clause 1.1 Clause 1.2.7 Clause 1.17 Annexure E Annexure F	<p>The Selected Bidder is required to adhere to the terms of this RFP document and any deviations to the same shall not be acceptable to UCO Bank.</p> <p>Incomplete bids or bids not conforming to the terms and conditions are liable for rejection by the Bank</p> <p>Acceptance of Terms A Recipient will, by responding to Bank RFP, be deemed to have accepted the terms as stated in the RFP.</p> <p>If our bid is accepted, we are responsible for the due performance as per the scope of work and terms & conditions as per mentioned in RFP.</p> <p>We hereby agree to comply with all the terms and conditions / stipulations as contained in the RFP and the related addendums...</p>	There are few terms and conditions in relation to which we would like to suggest changes and reach mutual consensus with the Bank. Hence, we submit that the contract to be signed between the Bank and the Bidder should be a mutually acceptable agreement, incorporating the terms of Bidder's proposal. Bidder is willing to conform and abide by the terms and conditions mentioned in the RFP except for such specific sections against which deviations are proposed by the Bidder.	Clause stands as per RFP
161	10	Clause 1.2.17	Further, subsequent to the orders being placed, the Bidder shall pass on to the Bank all fiscal benefits arising out of reductions in Government levies viz. Sales tax, excise duty, customs duty, etc.	<p>Finance & Solution - please check and confirm</p> <p>If there is any change in the taxation during contract period, recommended to consider at the prevailing rate at the time of billing/payment.</p>	Clause stands as per RFP
162	12	Clause 1.4	<p>Earnest Money Deposit</p> <p>1.4.2 - In the case of a successful bidder, if the bidder fails in accordance with any Terms and Conditions or any requirement as specified in this document.</p> <p>1.4.4 - The bidder violates any of the provisions of the terms and conditions of this tender specification.</p>	We submit that the EMD should be forfeited only if the Bidder fails to adhere to any mutually agreed terms and conditions of the contract.	Clause stands as per RFP

163	17	Clause 1.22	Indemnity The bidder shall indemnify the Bank and be liable for any loss or damage suffered by the Bank due to malfunctioning of the system as supplied and installed by them. The total liability of the selected bidder shall not exceed the total cost of the order value.	We submit that the indemnities required herein in both the referenced sections are too broad. We propose that the indemnities should be only in relation to the 3rd party claims for the following: a. Claims for loss or damage to third party tangible property; b. claim by any person in respect of personal injury or death; c. claims by any third party in respect of any IP infringement; and d. costs of defending or settling any of above claims. We also propose that the indemnity for death, personal injury and damage to tangible property should be mutual.	Clause stands as per RFP
	43	Clause 5.13	Indemnity	We submit that the word "indirectly" mentioned in clause 5.13 should be removed. We also propose that the provision of this clause 5.13 which requires the Vendor to provide indemnity for the claims made by customers, users and service providers of the Bank and/or regulatory authorities should be deleted.	
164	38	Clause 5.4	Performance Bank Guarantee	We propose that the Performance Bank Guarantee should be invoked only in the event bidder commits a material breach of the contract and fails to cure the same within 30 days of receipt of a written notice for cure.	Clause stands as per RFP
165	41	Clause 5.8	Liquidated Damages	We submit that the liquidated damages/penalty mentioned herein should be charged only if the delay is solely attributable to the Bidder. We also propose that the liquidated damages should be charged at the rate of 0.5% of the value of the delayed deliverables upto a maximum of 10% of the value of such delayed deliverables.	Clause stands as per RFP
166	43	Clause 5.12	Order Cancellation (• In case of cancellation of order, any payments made by the Bank to the Vendor would necessarily have to be returned to the Bank, further the Vendor would also be required to compensate the Bank for any direct	We submit that the provision pertaining to refund of payments mentioned herein should be deleted. It is also clarified that the compensation will be as decided by the competent courts, subject to liability limits agreed between the parties. We also propose	Clause stands as per RFP

		<p>Clause 5.19</p> <p>loss suffered by the Bank due to the cancellation of the contract/purchase order and any additional expenditure to be incurred by the Bank to appoint any other Vendor. This is after repaying the original amount paid.</p> <ul style="list-style-type: none"> • Vendor should be liable under this section if the contract/ purchase order has been cancelled in case sum total of penalties and deliveries equal to exceed 10% of the TCO.) <p>Exit Option and Contract Re-Negotiation</p> <p>(The Bank will reserve a right to re-negotiate the price and terms of the entire contract with the Selected Bidder at more favourable terms in case such terms are offered in the industry at that time for projects of similar and comparable size, scope and quality.)</p> <p>(The Bank shall have the option of purchasing the equipment from third-party suppliers, in case such equipment is available at a lower price and the Selected Bidder's offer does not match such lower price.)</p> <p>(Notwithstanding the existence of a dispute, and/or the commencement of arbitration proceedings, the Selected Bidder will be expected to continue the services.)</p> <p>(However, the Bank shall have the sole decision to ascertain whether such plan has been complied with)</p> <p>Termination</p>	<p>that this additional penalty of 10% of TCO is not relevant and should be removed.</p> <p>We submit that since this is a fixed duration and fixed priced contract, this provision stipulating for re-negotiation of price and terms is not relevant and should be deleted.</p> <p>We also propose for deletion of this provision. It is hereby clarified that the price is quoted for the entire solution and individual equipments cannot be purchased from any third party suppliers.</p> <p>We submit that the services that are the subject matter of dispute should be excluded. We agree to continue the services, except such services which are subject matter of the dispute. We submit that this provision which gives Bank the sole right to decide should be deleted.</p> <p>We propose that any order cancellation / exit option / termination provision should be invoked only for serious & material breaches. We also submit that the termination provision should be mutual and there should be a provision for adequate cure period prior to invocation of termination/ order cancellation / exit option provision. Hence we propose replacement of these clauses with the following: "Either party may terminate the contract if the other party commits a material breach of the contract (including non-payment of fees) and fails to cure the same within 30 working days of receipt of a written notice for cure."</p> <p>We also submit that the 1st para of clause 5.21 should be linked with the 2nd para. Accordingly, the notice period of 90 days should be followed by a cure period of 30 days.</p>	
		<p>Clause 5.21</p>		

167	45	Clause 5.17	<p>Guarantees</p> <p>(Selected bidder should guarantee that all the material as deemed suitable for the delivery and management of the Installation, Commission and Maintenance of This MPLS link scope as defined under this document, are licensed and legal. All hardware and software must be supplied with their original and complete printed documentation.)</p>	<p>We submit that the term "guarantee" as used herein is not relevant. It should be changed to "Warranty". We submit that we will pass on to Bank the warranties as provided by the respective OEMs/Licensors.</p>	Clause stands as per RFP
168	47	Clause 5.18	<p>Resolution of Disputes</p> <p>(Notwithstanding the above, the Bank shall have the right to initiate appropriate proceedings before any court of appropriate jurisdiction, should it find it expedient to do so.)</p>	<p>We submit that this provision should be made mutual. Either party shall have the right to initiate appropriate proceedings before any court of appropriate jurisdiction, should it find it expedient to do so.</p>	Clause stands as per RFP
169	50	Clause 5.22	<p>Effect of Termination</p> <p>In case the bank wants to continue with the Selected bidder's services after the completion of this contract/ purchase order then the Selected bidder shall offer the same or better terms to the bank. Unless mutually agreed, the rates shall remain firm.</p> <p>The Bank shall make such prorated payment for services rendered by the Selected bidder and accepted by the Bank at the sole discretion of the Bank in the event of clause of termination, provided that the Selected bidder is in compliance with its obligations till such date. However, no payment for "costs incurred, or irrevocably committed to, up to the effective date of such termination" will be applicable to Selected Bidder. There shall be no termination compensation payable to the Selected bidder.</p>	<p>We hereby submit that the duration of reverse transition services should be mutually discussed and included in the reverse transition plan in the contract.</p> <p>Solution team - please check and confirm</p> <p>We submit that the bidder should be paid for all the services rendered by the bidder. Hence, the provision stating "sole discretion of Bank" should be deleted.</p> <p>We also submit that the termination compensation if any will be as decided by the court of competent jurisdiction. Hence, the last sentence should be deleted.</p>	Clause stands as per RFP
170	51 96	<p>Clause 5.25</p> <p>Annexure I - Clause 7</p>	<p>Signing of Integrity Pact</p> <p>7. Fall Clause</p> <p>7.1 The BIDDER undertakes that it has not supplied/is not supplying similar product/systems or subsystems at a price lower than that offered in the</p>	<p>We submit that the Fall Clause should be modified as follows:</p> <p>"The BIDDER undertakes that it has not supplied/is not supplying identical product/systems or subsystems, as a part of the whole solution with the</p>	Clause stands as per RFP

			present bid in respect of any other Ministry/Department of the Government of India or PS U and if it is found at any stage that similar product/systems or sub systems was supplied by the BIDDER to any other Ministry/Department of the Government of India or a PSU at a lower price, then that very price, with due allowance for elapsed time, will be applicable to the present case and the difference in the cost would be refunded by the BIDDER to the BUYER, if the contract has already been concluded.	same scope and terms & conditions, during 6 months prior to the bid submission, at a price lower than that offered in the present bid in respect of any other Ministry/Department of the Government of India or PSU and if it is found at any stage in the bid process that identical product/systems or sub systems, as a part of the whole solution with the same scope and terms & conditions, was supplied by the BIDDER to any other Ministry/Department of the Government of India or a PSU at a lower price, then that very price, with due allowance for elapsed time, will be applicable to the present case and the difference in the cost would be adjusted at the time of contracting."	
171			Limitation of Liability (New clause)	<p>We propose that the below provision on limitation of liability should be included in the contract:</p> <p>"Limitation of liability: In no event will either party be liable for any indirect, incidental, special or consequential costs or damages; downtime costs; lost business, revenues, goodwill or profits; failure to realize expected savings; loss or unavailability of or damage to data or software restoration, even if such party has been advised of the possibility of such damages.</p> <p>Bidder's aggregate liability under this contract regardless of the form or nature of the action giving rise to such liability (whether in contract, tort or otherwise), shall be at actual and limited to the total contract value.</p> <p>Bidder will not be liable for any breach, which is caused by or otherwise attributable to any act or omission on part of Bank or third parties authorized by Bank, or on account of any force majeure event. In such event where Bank fails to perform its obligations, Bidder shall be (i) relieved from its own performance obligations, (ii)</p>	Clause stands as per RFP

				reimbursed for any costs incurred; and (iii) paid for additional service performed due to Bidder's failures or delays."	
172			Intellectual Property Rights (New Clause)	<p>We submit that the following provision should be included in the contract:</p> <p>"Each party shall retain ownership of its pre-existing Intellectual Property Rights ("Pre-existing IPR") and any improvements, up-gradations, enhancements, modifications and enhancements to and derivative works thereto;</p> <ul style="list-style-type: none"> • IPR ownership in any third party products provided by Bidder, and all improvements, up-gradations, enhancements, modifications and enhancements to and derivative works from such third party products shall remain with the respective third party. Nothing in this Agreement transfer any ownership or title in or to any Bidder or third party IPR. • Bank shall use the products in accordance with the license terms and restrictions specified by the OEM to be applicable for the use of such products. • Bank shall grant to the Bidder, at sole cost and expense of Bank, necessary rights and license to any intellectual property that is necessary for the Bidder and its designees to perform the services." 	Clause stands as per RFP
173	18	Part - II, Section 2.1 - Eligibility Criteria		<p>We would request the Bank to kindly add the following clause in its RFP as part of the Eligibility Criteria. "In case of corporate restructuring of a company (re-organization / separation / split / merger / spin-off), certificate of incorporation, financials & experience / credentials prior to such restructuring could be furnished along with the board resolution for restructuring."</p> <p>As you may be aware from Nov 1st 2015, we had a corporate restructuring exercise where in a new entity had been formed namely, Hewlett Packard</p>	Clause stands as per RFP

				Enterprise India Pvt Ltd. As all historical financial records would be based on HP India Sales Pvt Ltd, we would like this paragraph to be included so that we are allowed to put financial records of HP India Sales Pvt Ltd.	
174	18	Part - II, Section 2.1 - Eligibility Criteria	Documents to be submitted: Purchase order in name of bidder and execution certificate from existing customer(s).	Request you to kindly provide the option to bidders to provide the reference letters only. As sharing of PO copy may not be allowed as per the confidentiality agreement. Hence please change clause to: Purchase order in name of bidder or execution certificate from existing customer(s).	Clause stands as per RFP
175	18	Part - II, Section 2.1 - Eligibility Criteria	Point No. 6 The Proposed OEM's network equipment (all types) for datacenter should be running in a PSU Bank having minimum 2500 branches at time of submission of this RFP.	We understand that "all types" refer to "Routers and Switches Only". Pls confirm if our understanding is correct.	All network devices related to Datacenter (viz. Routers, Switches, Firewalls, IPS, Authentication System, Wan optimization).
176	18	Part - II, Section 2.1 - Eligibility Criteria	Point No. 5 - The bidder should have service/support center as per Annexure-H Point No. 6 - The bidder should not have been blacklisted /debarred for corrupt and fraudulent practices by Govt. organizations/Financial Institution /Bank as per RFP submission date.	There is a typo error in the sequence. These points should be 7 & 8.	Yes
177	76	IPS Technical Features, Point #4	Proposed IPS appliance should be supplied with minimum of 16 GB RAM and can be upgradable to 24 GB in future if required	IPS Appliances are supplied with custom built hardware that are signed for detection at wire speeds. RAM Upgrade indicates that the appliance may not be purpose built and built on regular hardware.	Please refer modified technical requirement of IPS in corrigendum
178	76	IPS Technical Features, Point #19	The average latency of the proposed IPS should be less than 150 microseconds	The appliance supports less than 40 MS. This should be factored and used as the baseline.	Please refer modified technical requirement of IPS in corrigendum
179	76	IPS Technical Features, Point #20	IPS must support a minimum of 5 million concurrent connections.	The appliance supports more than 60 million concurrent sessions and should be factored as the baseline.	Please refer modified technical requirement of IPS in corrigendum
180	77	IPS Technical Features, Point #24	IPS should have the functionality of Software Fail Open	The Appliance provide HA using Its Intrinsic and Transparent HA capabilities. It can permit or block traffic based on the configuration.	Please refer modified technical requirement of IPS in corrigendum

				Software based HA can have issues with the hardware failure as it may not allow the software to control the same.	
181	77	IPS Technical Features, Point #24	IPS Software Fail Open functionality can be defined in terms Gateway Threshold of Memory or CPU and should have an option to trigger the mail if required.	The Appliance provide HA using Its Intrinsic and Transparent HA capabilities. It can permit or block traffic based on the configuration. Software based HA can have issues with the hardware failure as it may not allow the software to control the same.	Please refer modified technical requirement of IPS in corrigendum
182	78-81	ANNEXURE –G, Required Minimum Technical Features of WAN Optimization,	Should have minimum 6 x 10/100/1000 Base-T Ports for inline deployment with fail-to-wire capability. In total 6 ports are required from day one	This clause restricts us to participate in the bid. Kindly amend the clause as " Should have minimum 4 x 10/100/1000 Base-T Ports for inline deployment with fail-to-wire capability. In total 4 ports are required from day one	Please refer modified technical requirement of WAN Optimization in corrigendum.
183	78-81	ANNEXURE –G, Required Minimum Technical Features of WAN Optimization,	The Appliance should able to peer with multiple type of remote devices including, Appliance, Virtual Appliance, Router integrated WAN Optimization solution etc.	Specific to one OEM. Please remove this clause	Please refer modified technical requirement of WAN Optimization in corrigendum.
184	10 38	1.2 Submission of Bid 5.5 Price	1.2.14 The bidder is required to guarantee that exchange rate fluctuations, changes in import duty and other taxes will not affect the Rupee value of the commercial bid over the price validity period. 1.2.17 Further, subsequent to the orders being placed, the Bidder shall pass on to the Bank all fiscal benefits arising out of reductions in Government levies viz. Sales tax, excise duty, custom duty, etc. The cost of network link must include rental charges of network equipment's e.g modem, repeater, etc. required to be terminated the link at CPE Ethernet interface. The Price Bid also must include all applicable taxes such as Sales/Service/VAT / Waybill etc. The Octroi /Entry Tax will be paid extra, wherever applicable on submission of actual Tax receipt. The Selected bidder is required to guarantee that exchange rate fluctuations, changes in import duty and other taxes will not affect the Rupee value of the commercial bid, over the validity period of the bid.	In case of any variation (upward or downward) in applicable taxes, excise, custom duty or government levies which are deemed to have been included as part of the price, or a new type of tax, duty or levy (like GST etc.) is introduced during the term of the contract, the Vendor's quoted price will be increased or decreased by an amount reflecting the changes.	Clause stands as per RFP

			Prices quoted by the selected bidder shall be in Indian Rupees, firm and not subject to any price escalation, if the order is placed within the validity period. Further, subsequent to the orders being placed/agreement executed, the selected bidder shall pass on to the Bank all fiscal benefits arising out of reductions in Government levies viz. Sales tax, excise duty, custom duty, etc.		
185	38	5.4 Payment Terms	5.4.2 90% of the value of new network equipment/devices/solutions/link implementation/shifting/upgradation of along with Taxes, will be paid after delivery and completion of successful installation & operational, on submission of proof of delivery and the acceptance certificate duly signed by Bank's authorized official & satisfactory service report from the Bank where the systems have been installed after realizing penalty charges for late delivery & installation, if any. The balance 10% of order value will be paid after 3 months successful running.	Request the bank to kindly replace this with proposed clause. 5.4.2 90% 100% of the value of new network equipment/devices/solutions/link implementation/shifting/upgradation of along with Taxes, will be paid after delivery and completion of successful installation & operational, on submission of proof of delivery and the acceptance certificate duly signed by Bank's authorized official & satisfactory service report from the Bank where the systems have been installed after realizing penalty charges for late delivery & installation, if any. The balance 10% of order value will be paid after 3 months successful running.	Clause stands as per RFP
186	40	5.7 Payment against delivery of SLAs :	Bank will pay charges on per site basis depending upon the achievement of uptime.	We submit that the penalties should be applicable only in the events the delay/default is solely and entirely attributable to the Vendor. We request that the overall cap for all the penalties should be limited to 5% of the monthly Facility Management service charges.	Clause stands as per RFP
187		New	Invoicing Terms	We submit that payment should be made within 30 days from the date of invoice. Also any dispute shall be raised within reasonable time not more than 7 days from receipt of invoice.	Clause stands as per RFP
188		New	NA	Request to provide excel based pricing template	Clause stands as per RFP
189	Part II - 2.1 (4)	Part II - 2.1 (4)	The Bidder should have involved in Supply,	Request to change the clause as, "The Bidder should have involved in Supply,	Clause stands as per RFP

	/ page no. 18		Installation, Configuration & Maintenance of Network devices (Software and Hardware), management & monitoring of MPLS/P2P and ISDN links and providing related services for at least 5 years in 2 nos. of Govt. Financial Institution/Bank in India having minimum 2500 branches/office network in each organization, out of which one should be Public Sector Bank.	Installation, Configuration & Maintenance of Network devices (Software and Hardware), management & monitoring of MPLS/P2P and ISDN links and providing related services for at least 5 years in 2 nos. of Govt. Financial Institution/Bank in India having minimum 1000 branches/office network in each organization, out of which one should be Public Sector Bank." reason being customer many times purchase network devices deparately and MPLS /P2P links separately. Both should not be linked together. The UCO banks existing network also has two separate OEMS (cisco and HP) for routers.	
190	Part II - 2.1 / page no. 18	Part II - 2.1 (5)	The Proposed OEM's network equipment for branches (Router & Switch) should be running in 1500 branches in a Public Sector Bank at time of submission of this RFP.	Reques to the change the clause as,"Any reputed OEM's (OEM should be in Gartner's Magic Quadrant in 2015) network equipment for branches (Router and/ or Switch) should berunning in 1000 branches in a Public Sector Bank at time of submission of this RFP." reasons being (1) for MPLS connectivity only routers are required and switches are used in the office LAN network (2) OEMs can be different with different customers and RFP should not bind the bidder with only one OEM. The UCO banks existing network also has two separate OEMS (cisco and HP) for routers.	Clause stands as per RFP
191	Page No. 215 and other locations		Make and model Nos of Routers and other devices	Request to provide the Serial Numbers of all the branch , HO, Core Network devices and DC routers and other devices so that we can offer the cost effective AMC for these existing items.	Clause stands as per RFP
192	Page No. 215		Ageing Details of Routers and other devices	Please provide the date of commissioing , current warranty details and ageing details on all the routers	Clause stands as per RFP

	and other locations			and /or modems and other devices so that we can offer cost effective solutions.	
193	40	5.7 Payment against delivery of SLAs	Bank will pay charges on per site basis depending upon the achievement of uptime. i.e.. => Uptime = Less than 95%. AND % of Payment = NIL.	Request to add a clause on upper limit of Penalty as , " The total penalty charges in a year can be maximum of 10% of the total of Annual Network Management Service charges for all the locations".	Clause stands as per RFP
194	10	Part I, Clause no. 1.2.14	The bidder is required to guarantee that exchange rate fluctuations, changes in import duty and other taxes will not affect the Rupee value of the commercial bid over the price validity period.	If there is any change in the exchange rate during contract period, recommended to consider at the prevailing rate at the time of billing/payment.	Clause stands as per RFP
195	10	Part I, Clause no. 1.2.17	Further, subsequent to the orders being placed, the Bidder shall pass on to the Bank all fiscal benefits arising out of reductions in Government levies viz. Sales tax, excise duty, custom duty, etc.	If there is any change in the taxation during contract period, recommended to consider at the prevailing rate at the time of billing/payment.	Clause stands as per RFP
196	11	Part I, Clause no. 1.2.20	The Bank reserves the right to modify any terms, conditions and specifications of this request for submission of offer and to obtain revised bids from the bidders with regard to such changes. The Bank reserves its right to negotiate with any or all bidders. The Bank reserves the right to accept any bid in whole or in part.	In case of any such modification if any cost impact or time schedule will be required to modify that should be considered .	Clause stands as per RFP
197	20	Part IV, Clause no, 4.2	Contract Duration: Initially for a period of three year from 01/01/2017 and extendable for a further period of 2 years subject to satisfactory performance.	In case of extension of the contract period, Recommended to consider revised price with agreed mutual consent between both the parties.	If, extended mutually decided terms & conditions.
198	30	Part IV, Clause no. 4.19	Bidder Deliverables and Liability: ii) Required manpower should be deputed at Bank DC & DR site within 1 weeks from the date of Purchase Order. viii)Dedicated Shared resources to be deployed at all 20 ZO's Locations. Details of shared resources will be submitted to Bank within one week from the date of award of contract.	Recommended modifications as under: ii) Required manpower should be deputed at Bank DC & DR site within 6 weeks from the date of Purchase Order. viii)Dedicated Shared resources to be deployed at all 20 ZO's Locations. Details of shared resources will be submitted to Bank within 6 weeks from the date of award of contract.	Clause stands as per RFP

199	32	Part IV, Clause no. 4.22 (i)	The advanced level training programme shall be held in bank's different HO/Zonal training centre located across the country for the network user at, DC, DRs and ZO other offices. The training shall be related to LAN, WAN, networking equipment etc.	Who will bear the training cost? Requested to clarify the same.	Clause deleted.
200	37	Part V, Clause no. 5.3.1	Deliveries of the new networks equipment/device/solution, installation and operationalization of complete solution at all locations should be made within 4 weeks from the date of purchase order.	Deliveries of the new networks equipment/device/solution, installation and operationalization of complete solution at all locations should be made within 8 weeks from the date of purchase order.	Clause stands as per RFP
201	37	Part V, Clause no. 5.3.2	Bidder has to commission the links at DC and DR within 4 weeks and all other links within 6 weeks.	Recommended modifications as under: Bidder has to commission the links at DC and DR within 6 weeks and all other links within 8 weeks.	Clause stands as per RFP
202	37	Part V, Clause no. 5.3.4	Shifting/upgradation of link will be completed within 4 weeks from date of PO for shifting the link.	Requested to provide duration of 6 weeks from the date of PO for Shifting/upgradation of link.	Clause stands as per RFP
203	38	Part V, Clause no. 5.4.2	90% of the value of new network equipment/devices/solutions/link implementation/shifting/upgradation of along with Taxes, will be paid after delivery and completion of successful installation & operational, on submission of proof of delivery and the acceptance certificate duly signed by Bank's authorized official & satisfactory service report from the Bank where the systems have been installed after realizing penalty charges for late delivery & installation, if any. The balance 10% of order value will be paid after 3 months successful running.	Recommended modifications as under: i) 70% on delivery ii) 20% on installation iii) 10% on Go-live	Clause stands as per RFP
204	38	Part V, Clause no. 5.4.4	Payment towards Facility Management & AMC will be made quarterly in arrears after issuing of necessary invoice and submission of monthly reports including SLA and after deduction of penalties if any. In case of termination of services, the payment will be made on pro rata basis for the duration for which the services were provided.	Requested to provide payments towards Facility Management & AMC on monthly basis.	Clause stands as per RFP
205	41	Part V, Clause no. 5.8	Any delay in delivery/installation/commissioning/shifting/upgradation of the link/device/equipment/solution	Requested to keep the maximum LD cap of 5% on the delayed portion.	Clause stands as per RFP

			<p>beyond the stipulated time period as per clause no. 5.3, Bank will charge penalty at 1 % of the order value for that link/device/equipment/implementation cost per week or part thereof, subject to a maximum of 10%. The bank may at its discretion also waive or reduce the penalty if the reasons for delay are considered to be justified. After elapsing of stipulated time period including 10 Weeks Liquidated damages period, if selected bidder fails to implement any or all MPLs link in branches, the order for such links will be deemed cancelled after imposing necessary penalty amount as per LD clause 5.8 and bank will place the order to any other selected bidder.</p> <p>If Bidder fails to commission the link as per feasibility report (this includes change of media) 10% of the link cost will be deducted from payment of other link or from Performance Bank Guarantee and bank will place the order to any other selected bidder.</p>		
206			Maximum Penalty	Requested to keep the maximum penalty cap of 5% of opex /O&M value of contract	Clause stands as per RFP
207	12	1.4	<p>Earnest Money Deposit</p> <p>The Bidder must submit Earnest Money Deposit (EMD) along with the Technical Bid in the form of Bank Guarantee having validity period for 1 year from the date of opening of Technical Bid in the format given in Annexure D. The EMD amount is ` 50 Lac (Rupees Fifty Lac Only) issued by any scheduled Commercial bank</p>	<p>Earnest Money Deposit</p> <p>The Bidder must submit Earnest Money Deposit (EMD) along with the Technical Bid in the form of Bank Guarantee having validity period for 4 month from the date of opening of Technical Bid in the format given in Annexure D. The EMD amount is ` 50 Lac (Rupees Fifty Lac Only) issued by any scheduled Commercial bank</p>	Clause stands as per RFP
208	38	5.5	<p>Price</p> <p>The cost of network link must include rental charges of network equipment's e.g modem, repeater, etc. required to be terminated the link at CPE Ethernet interface. The Price Bid also must include all applicable taxes such as Sales/Service/VAT / Waybill etc. The Octroi /Entry Tax will be</p>	In case of any increase /decrease of tax rate or introduction any new tax during contract period , it would be recommended to consider prevailing rate of taxes applicable at the time of billing /payment	Clause stands as per RFP

			paid extra, wherever applicable on submission of actual Tax receipt.		
209	38	5.5	The Selected bidder is required to guarantee that exchange rate fluctuations, changes in import duty and other taxes will not affect the Rupee value of the commercial bid, over the validity period of the bid. The prospective service provider shall establish the Network and should be capable of maintaining it for a minimum period of 3 years initially and then subsequent extension for 2 years based on performance basis.	In case of any such expenses it would be recommended to consider prevailing rate during contract period	Clause stands as per RFP
210	60	Router Type A (3)	Should have at least 1 Nos. 10/100/1000 Mbps Ethernet interfaces.	Please specify if 1 No.s 10/100/1000Mbps port is required in addition to 2 No. of WAN Ports. Also these additional ports will be used to connect to the Core/Distribution switch i.e. for connecting to LAN Network	Please refer modified technical requirement of router in corrigendum
211	60	Router Type A (4)	Should have at least 2 No. of Gigabit Ethernet WAN Port.		
212	62	Router Type B (3)	Should have at least 2 Nos. 10/100/1000 Mbps Ethernet interfaces.	Please specify if 2 No.s 10/100/1000Mbps port is required in addition to 2 No. of WAN Ports. Also these additional ports will be used to connect to the Core/Distribution switch i.e. for connecting to LAN Network	Please refer modified technical requirement of router in corrigendum
213	62	Router Type B (4)	Should have at least 2 No. of Gigabit Ethernet WAN Port.		
214	62	Router Type C (3)	Should have at least 3 Nos. 10/100/1000 Mbps Ethernet interfaces.	Please specify if 3 No.s 10/100/1000Mbps port is required in addition to 2 No. of WAN Ports. Also these additional ports will be used to connect to the Core/Distribution switch i.e. for connecting to LAN Network	Please refer modified technical requirement of router in corrigendum
215	62	Router Type C (4)	Should have at least 2 No. of Gigabit Ethernet WAN Port.		
216	65	Switch Type A (1)	Chassis based & modular architecture for scalability and should be a single box configuration for ease of management.	Would request to change the clause and remove the " chassis based architecture" since only 24 port's is required and considering the ports requirement, chassis based architecture will introduce the need of higher end switch which would be an overkill	Please refer modified technical requirement of switch in corrigendum
217	65	Switch Type A (2)	Switch should have minimum 150 Gbps Switching capacity all the services enabled on switch.	Would request to change the throughput to 50 Gbps, since with 24 Gig Ports and 2 Uplinks 150 Gbps is an overkill	Please refer modified technical requirement of switch in corrigendum
218	66	Switch Type A (12)	Should support NAT, PAT, DHCP	Kindly request to remove NAT from the feature list, as this feature is required in gateway routers and not switches	Please refer modified technical requirement of switch in corrigendum
219	70	Firewall (9)	Required Minimum Technical Features of Firewall	Please clarify how this need to be validated?	Please refer modified technical requirement of firewall in

					corrigendum
220	68	Firewall (9)	Firewall performance should be minimum 20 Gbps (realworld throughput)	Please clarify if 20 Gbps throughput is required with all the features turned on i.e. (IPS, AMP, AVC and URL Filtering)	Please refer modified technical requirement of firewall in corrigendum
221	68	Firewall (9)	Support for minimum 1000 MAC addresses	MAC address support is required to be used for which feature	Please refer modified technical requirement of firewall in corrigendum
222	67	Firewall (9)	The appliance should be capable of providing Firewall, VPN Services and Next Generation Firewall feature	What all next generation features are required to be enabled from day one? If remote VPN is required, kindly mention the no of users licenses	Please refer modified technical requirement of firewall in corrigendum
223	74	Firewall (9)	The management platform must be accessible via a web-based interface and ideally with no need for additional client software.	This is not secure and specific to few OEMs. Please remove	Please refer modified technical requirement of firewall in corrigendum
224	82	Proxy	The solution should be a on premise Secure Web Gateway solution having Proxy, user based URL filter, user based Application filtering on mobile devices like blocking of WhatsApp, Caching, SSL Inspection, Anti-Virus, Antimalware, spyware blocking, blocking of Peer-Peer applications like Kazaa, Gnutella, Bit Torrent, IRC (over HTTP) , including blocking of voice and video services and real-time protection against zero day threats all in one solution(Appliance or software installed in Server).	Does features like SSL inspection should be working from day one?	Yes
225	82	Proxy	The solution must Appliance based or run on physical servers and support minimum of 500 concurrent users from the day one and scalable up to 4000 concurrent users without changing hardware.	Should hardware be factored to support 4000 concurrent user from day one? No of user licensed to be factored as 500, for rest 500*7 licenses only cost to be provided?	Please refer modified technical requirement of proxy in corrigendum
226	102	Proxy	Upgradation hardware for additional 2000 concurrent user		
227	102	Proxy	License Cost for 500 user licenses block		
228	76	IPS	The IPS should be able to inspect SSL/https traffic	Does features like SSL/HTTPS inspection should be working from day one?	Yes
229	76	IPS	The proposed device should have Intrusion prevention sensors delivering a minimum of 10 Gbps of context-aware , real-world traffic inspection	Please clarify whether this throughput performance is considering bi-directional scanning and customized profiling	Please refer modified technical requirement of proxy in corrigendum
230	21	PART –IV SCOPE OF WORK	Management includes proactive monitoring, performance management, problem management and change management and everything else necessary for effective	Does Bank will provide in house toll to do the proactive monitoring?	Yes. HP Open View (NNM)

			functioning of the WAN as per the service levels		
231	21	PART –IV SCOPE OF WORK	The bidder will provide for the management of the entire WAN including managing network 259connection devices such as routers, switches, Firewall, IPS/IDS, VPN devices etc. and all types of network links such as MPLS, leased line, ISDN, CDMA and VSAT as also migration /upgradation/implementation- of the Network Links	Does Bidder has to co-ordinate with the Private Service provider also? Does private SP will have any onsite support for their link management?	Bidder should coordinate with ISP link as per Annexure L
232	23	4.1 Summary of the Requirement	Monitoring and management of WAN network using NMS tools	Does Bank already having working NMS tool?	HP Open View (NNM)
233	23	4.1 Summary of the Requirement	Support service for ATM Switch	Please provide the details of ATM switch. Does this support refers the comprehensive support?	Please refer 4.1 clause in corrigendum
234	23	4.1 Summary of the Requirement	AMC of network equipment at DC, DR site, Head Offices, Zonal Offices, Branches as per Annexure -L	What is the Bank expectation if any device under AMC declared EoL by the OEM before the AMC contract period?	Please refer warranty clause in corrigendum
235	23	4.2 Baselines	Initially for a period of three year from 01/01/2017 and extendable for a further period of 2 years subject to satisfactory performance.	Is this applicable for New purchase only or for AMC devices also?	Yes
236	23	4.2 Baselines	24x7 for Network link Monitoring, 24x7 for Network Management support.	Is this on-site support or mean remote support?	Onsite support as per clause no 4.3
237	24	4.4 WAN Network Monitoring	Provide monthly Site up time reports. Link and device availability reports.	Expected report would be generated from the Bank's on-site tool and no separate tool will be require from the Bidder's side.	
238	25	4.4 WAN Network Monitoring	Backup of device configurations on a weekly basis as per policy defined by Bank.	Expected necessary storage will be provided by the Bank.	Yes
239	27	4.9 Maintenance of existing Networking Equipment	Successful Bidder has to maintain the equipments supplied by him and the equipments under AMC with him and keep sufficient spare parts for maintaining the uptime of the equipment/site	Does Bank is asking for on-site spare?	No.
240	27	4.9 Maintenance of existing Networking Equipment	Will be responsible for ensuring preventive maintenance	Is there any guideline for the PM activity?	No.
241	27	4.9 Maintenance of existing Networking Equipment	Successful Bidder shall be responsible for maintaining the branch LAN up to branch switch level	Does this include LAN passive part alose or only the switch?	Successful Bidder shall be responsible for maintaining the branch LAN up to branch switch level
242	28	4.12 Uptime maintenance	Uptime maintenance	does this mean network/ solution or device?	

243	28	4.13 Integration of new application/network on existing Network	Bank may implement new applications over the network. The successful Bidder shall implement such application/network for which it has to prepare plan, bandwidth sizing & identify network equipment specification for the integration.	What exactly mean by the application? Please elaborate.	New application for business and employee.
244	28	4.18 Helpdesk	Daily reports & monthly report.	Does Bank will provide necessary tools for the reporting?	No.
245		Last date of submission	19-10-2016	Request you to extend to 28-10-2016.	Clause stands as per RFP
246		4.19	ii) Required manpower should be deputed at Bank DC & DR site within 1 weeks from the date of Purchase Order.	We request 6 weeks time to deploy manpower	Clause stands as per RFP
247		Payment terms	5.4.2 90% of the value of new network equipment/devices/solutions/link implementation/shifting/upgradation of along with Taxes, will be paid after delivery and completion of successful installation & operational, on submission of proof of delivery and the acceptance certificate duly signed by Bank's authorized official & satisfactory service report from the Bank where the systems have been installed after realizing penalty charges for late delivery & installation, if any. The balance 10% of order value will be paid after 3 months successful running.	We request that payment for new equipment is processed as under: 1. 70% on delivery of material at site 2. 20% after implementation 3. Balance 10% after 3 months of successful running or in advance on submission of BG	Clause stands as per RFP
248		5.6 SLA	Exclusions and assumptions	Network unavailability due to ISP controlled activities will not be considered for downtime calculation for SLA	Bidder should maintain SLA as per 5.6 in corrigendum
249		5.7 Payment against SLA		We request the bank to put an overall cap of 15% of the monthly charges payable against support services for all sites.	Clause stands as per RFP.
250		5.12	In case of cancellation of order, any payments made by the Bank to the Vendor would necessarily have to be returned to the Bank, further the Vendor would also be required to compensate the Bank for any direct loss suffered by the Bank due to the cancellation of the contract/purchase order and any additional expenditure to be	Bidder request the bank to delete this clause. As per the payment terms all payment is being released only after successful completion of the given activity. Bidder will not be in position to refund any payment received for services/ products already delivered and committed.	Clause stands as per RFP

			incurred by the Bank to appoint any other Vendor. This is after repaying the original amount paid.		
251		5.19	The Bank will reserve a right to re-negotiate the price and terms of the entire contract with the Selected Bidder at more favourable terms in case such terms are offered in the industry at that time for projects of similar and comparable size, scope and quality.	We request that bidder is being selected through RFP process and discovery of lowest price and hence during the term of the contract bidder should not be subject to renegotiation unless mutually accepted.	Clause stands as per RFP
252			As aforesaid the Bank would procure the equipment from the third party only in the event that the equipment was available at more favourable terms in the industry, and secondly,	We request the bank to delete this clause as bidder is being selected through RFP process and discovery of lowest price and hence during the term of the contract third party should not be called to buy contracted quantity.	Clause stands as per RFP
253		Taxes		We request the bank to consider the following: 1. Taxes submitted with the bid shall be indicative and at the rates applicable on the day of submission of bids. However any change in rates or new taxes introduced by government shall be on bank's account 2. Bid price shall be exclusive of Octroi/entry taxes and the same shall be extra as applicable and paid at actual by the bank on production of necessary documents	Clause stands as per RFP
254		1	5.13 Indemnity – Page 43	RFP at various places requires bidders to indemnify and the indemnification obligation is very broad and without providing the detailed and established norms for indemnification. To make the contract reasonable and commercially viable as per standard practice observed within the industry, we request that the clarity be provided in the agreement that Indemnity shall only be restricted to third party claim for (i) IPR Infringement indemnity, and (ii) bodily injury and death and tangible property damage due to gross negligence and willful misconduct. The process of indemnification shall provide the requirement of notice, right to defend and settle, and the concept of apportionment (liable only to the extent of its claim), mitigation and	Clause stands as per RFP

				carve-outs.	
255		2	1.22 Indemnity – Page 17	RFP lacks clarity on entire liability of bidder under this RFP. Bidder requests that clarity be brought by including following limitation of liability clause in the RFP: "Neither Bank nor the Vendor shall in any event be liable for indirect and consequential loss and damages including but not limited to loss of business, anticipated revenue, loss of profit etc. To the extent allowed by laws in India, the liability of each party under this agreement, in any event regardless of nature of claim under contract, torts and other theory shall be limited to the total contract value under the purchase order."	Clause stands as per RFP
256		3	4.20 Covenant of the Bidder – Page 31	Bidder request that any audit by Bank shall be subject to certain security and confidentiality restrictions applicable to Bidder's premises or other client's data.	Clause stands as per RFP
257		4	Annexure –I - PRE CONTRACT INTEGRITY PACT – Fall Clause – Page 96	Price is always dependent on various factors and some of them are identified below. The integrity pact is for ensuring that bidders don't indulge in unethical behavior and ensuring competitiveness. The undertaking above shall not be applicable and we request that this clause is deleted.	Clause stands as per RFP
258				If Bank is not keen to delete the clause we kindly request Bank to clarify:	Clause stands as per RFP
259				i) That the undertaking above is only applicable if all other factors are identical.	Clause stands as per RFP
260				a) payment terms (advance or arrears or 30 days to 90 days payment terms)	Clause stands as per RFP
261				b) supply on best effort basis as against supply with liquidated damages and the rate of LD	Clause stands as per RFP
262				c) commercial and legal risk elements in contract	Clause stands as per RFP
263				d) place of supply (supply in centralized model as against decentralized model or supply in metros as against remote location)	Clause stands as per RFP
264				e) volume	Clause stands as per RFP
265				f) discount offered by OEM	Clause stands as per RFP
266				ii) that in the event the bidder doesn't have a control over price due to reason beyond its control (percentage	Clause stands as per RFP

				of discount provided by OEM) the same shall be taken into account.	
267				iii) that in case bidder doesn't have a tracking mechanism for tracking price, bidder shall be allowed to make such declaration.	Clause stands as per RFP
268				iv) that the clause shall only be effective prospectively and not retrospectively.	Clause stands as per RFP
269				v) that this kind of undertaking may have adverse impact on competition and in the event this is treated as anti-competitive the bidder shall not be liable.	Clause stands as per RFP
270	18	2.1 Eligibility Criteria >> Point 4	The Bidder should have involved in Supply, Installation, Configuration & Maintenance of Network devices (Software and Hardware), management & monitoring of MPLS/P2P and ISDN links and providing related services for at least 5 years in 2 nos. of Govt. Financial Institution/Bank in India having minimum 2500 branches/office network in each organization, out of which one should be Public Sector Bank.	Request Bank to change the clause as below: - The Bidder should have involved in Supply, Installation, Configuration & Maintenance of Network devices (Software and Hardware), management & monitoring of MPLS/P2P and ISDN links and providing related services for the last 5 years in 2 nos. of Govt. Financial Institution/ BFSI in India having minimum 1500 branches/office network in each organization, out of which one should be Public Sector Bank.	Clause stands as per RFP
271	24	4.3 On site Manpower Assignment >> Point ii	Bank Mentioned that resource is required for 24/7 and respective count is mentioned as 3. Similarly, One resource in General Shift	Our understanding is that, bank need 24/7 support with 1 resource in each shift however total number of support engineer will be more than 3 so as to provide leaves. Similarly in case of general shift, we assume that we need to deploy two engineers to maintain the shift from 8 AM to 8 PM. Kindly clarify whether our understanding is correct or not.	Clause stands as per RFP

Sl. No.	Para, Clause no., Page No.	Clause Details in RFP	Modified clause based on reply to Pre bid quires
1	CONTENTS Page 6	ANNEXURE - L1038 ANNEXURE - M1031	ANNEXURE - L109 ANNEXURE - M215
2	Part IV Clause no. 4.1 Page 22	<p><u>Summary of the Requirement</u> Following are the services required by Bank which will be provided by the bidder:</p> <p>i) Support the Wide Area Network infrastructure of Bank across India and overseas.</p> <p>ii) Monitoring and management of WAN network using NMS tools.</p> <p>iii) Configuration and fault management for the routers, switch, Firewall, IPS/IDS, VPN devices etc.</p> <p>iv) Support services for routers, switch, and security devices at the core distribution and access WAN locations.</p> <p>v) Support services for BSNL/MTNL MPLS, lease lines, ISDN lines, CDMA, Internet VPN, 84 Mbps point to point link & 16 Mbps MPLS backhaul link form TCL.</p> <p>vi) Support service for ATM Switch is connected from BDC and KDC through MPLS to Euronet Mumbai & Chennai datacenter using 4 Nos. of TCL link and 3 Nos of Sify link.</p> <p>vii) Support service for 2 no. of M/s Reliance and 1 no. of M/s TCL link at Mumbai Treasury for Western Grid CTS.</p> <p>viii) AMC of network equipment at DC, DR site, Head Offices, Zonal Offices, Branches as per Annexure -L</p> <p>Bank also have link (MPLS & VSAT) form other service (Except BSNL/MTNL). For said links monitoring Bank already have support team from respective service provider. Bidder should coordinate with ISP support team of link implementation, troubleshooting and smooth functioning.</p>	<p><u>Summary of the Requirement</u> Following are the services required by Bank which will be provided by the bidder:</p> <p>i) Support the Wide Area Network infrastructure of Bank across India and overseas <u>as per Annexure L</u></p> <p>ii) Monitoring and management of WAN network using NMS tools.</p> <p>iii) Configuration and fault management for the routers, switch, Firewall, IPS/IDS, VPN devices etc.</p> <p>iv) Support services for routers, switch, and security devices at the core distribution and access WAN locations.</p> <p>v) Support services for BSNL/MTNL MPLS, lease lines, ISDN lines, CDMA, Internet VPN, <u>2 no. of 84 Mbps point to point link from BSNL & TCL.</u></p> <p>vi) AMC of network equipment at DC, DR site, Head Offices, Zonal Offices, Branches as per <u>Annexure -M & J</u></p> <p>Bank also have link (MPLS & VSAT) form other service (Except BSNL/MTNL). For said links monitoring Bank already have support team from respective service provider. Bidder should coordinate with ISP support team of link implementation, troubleshooting and smooth functioning.</p>
3	Part IV Clause no. 4.9 Page 27	<p><u>Maintenance of existing Networking Equipment</u> i) The successful Bidder shall also maintain the existing network equipment deployed in the bank WAN.</p> <p>ii) Successful Bidder has to maintain the equipments supplied by him and the equipments under AMC with him and keep sufficient spare parts for maintaining the uptime of the equipment/site</p>	<p><u>Maintenance of existing Networking Equipment</u> i) The successful Bidder shall also maintain the existing network equipment deployed in the bank WAN <u>as per Annexure -M & J</u></p> <p>ii) Successful Bidder has to maintain the equipments supplied by him and the equipments under AMC with him and keep sufficient spare parts for maintaining the uptime of the equipment/site</p> <p>iii) <u>Turnaround time of spare parts should be 4 hours for DC, DR site, Mumbai Treasury and next working days for branches/office.</u></p>
4	Part IV Clause no. 4.12 Page 28	<p><u>Uptime maintenance</u> i) The overall uptime should be 99.9% Core network (DC, DR, HOs, Treasury, ATM Switch network)</p> <p>ii) The overall network uptime should be 99.5 % during business hours (8 am to 8 pm) for all days.</p> <p>iii) The overall network uptime should be 99% during non-business hours (8 pm to next day 8 am).</p>	<p><u>Uptime maintenance</u> i) The overall uptime should be 99.9% Core network (DC, DR)</p> <p>ii) The overall network uptime should be 99.5 % during business hours (8 am to 8 pm) for all working days <u>for all branches/offices except rural branch.</u></p> <p>iii) The overall network uptime should be <u>98% during business hours (8 am to 8 pm) all working days for rural branches.</u></p> <p>iv) To prevent site down due to failure of dual link or equipment, Successful</p>

		<p>iv) To prevent site down due to failure of dual link or equipment, Successful Bidder shall have to maintain the site uptime as specified in the uptime clause.</p> <p>v) No down time (site) shall be permitted in case of DC. DR Site will act as DC at the time of DC disaster as per DRP (Disaster Recovery Plan).</p> <p>vi) No down time (site) shall be permitted in case of DR site.</p>	<p>Bidder shall have to maintain the site uptime as specified in the uptime clause.</p> <p>v) No down time (site) shall be permitted in case of DC. DR Site will act as DC at the time of DC disaster as per DRP (Disaster Recovery Plan).</p> <p>vi) No down time (site) shall be permitted in case of DR site.</p>
5	Part IV Clause no. 4.11 (ii) Page 28	<p>Managing & Supporting Network at Help Desk level</p> <p>ii) The support at help desk level should be available during business hours (8.00AM to 8.00PM)for all 20 ZOs.</p>	<p>Managing & Supporting Network at Help Desk level</p> <p>ii) The support at help desk level should be available during business hours <u>(10.00AM to 7.00PM)</u>for all 20 ZOs.</p>
6	Part IV Clause no. 4.19 Bidder Deliverables and Liability (iv) & (v) Page 30	<p>iv) The onsite team shall maintain attendance register and the same should be sent monthly to Bank for SLA calculations, failing which appropriate penalty condition as defined below shall be invoked.</p> <p>v) The onsite team shall not be changed without adequate notice (minimum 15 days) to Bank. Any resigned resource of onsite team should not be relieved before giving suitable replacement. Any breach of this clause will attract penalty</p>	<p>iv) <u>The onsite team shall maintain attendance register and the same should be sent monthly to Bank.</u></p> <p>v) The onsite team shall not be changed without adequate notice (<u>minimum 30 days</u>) to Bank. Any resigned resource of onsite team should not be relieved before giving suitable replacement. Any breach of this clause will attract penalty.</p>
7	Part IV Clause no. 4.22 Page 32	<p><u>Training & support for product evaluation</u></p> <p>i) The advanced level training programme shall be held in bank's different HO/Zonal training centre located across the country for the network user at, DC, DRs and ZO other offices. The training shall be related to LAN, WAN, networking equipment etc.</p> <p>ii) For user level training programme, Successful Bidder shall have to provide faculty at different training programme organised by bank at bank's different Zonal training centre located across the country.</p> <p>iii) The successful Bidder shall provide support on evaluation of new trends/technology in the networking, network security, and network performance enhancement for betterment of banks' network.</p> <p>iv) The Successful Bidder shall suggest optimal utilisation and expansion of network.</p> <p>v) The Successful Bidder shall coordinate with the banks' security consultant / security integrator for ensuring network security.</p> <p>vi) The Successful Bidder shall coordinate with the banks' IT consultant / advisors for evaluating any network related issues.</p>	<p><u>Support for product evaluation</u></p> <p><u>i) The successful Bidder shall provide support on evaluation of new trends/technology in the networking, network security, and network performance enhancement for betterment of banks' network.</u></p> <p><u>ii) The Successful Bidder shall suggest optimal utilisation and expansion of network.</u></p> <p><u>iii) The Successful Bidder shall coordinate with the banks' security consultant / security integrator for ensuring network security.</u></p> <p><u>iv) The Successful Bidder shall coordinate with the banks' IT consultant / advisors for evaluating any network related issues.</u></p>
8	Part IV Clause no. 4.57 Page 35	<p>IP scheme management including IPv6</p>	<p>IP scheme management including IPv6. <u>Bidder should migrate whole/partial network into IPv6 in future if required through a separate process.</u></p>
9	Addition in Part IV		<p><u>Part IV Scope of work Clause No. 4.73</u></p> <p>At present core firewall FWSM (WS-SVC-FWM-1-K9) is Cisco OEM make (Sl. no. 7, Table F, Annexure J), will be replace with ASA Services Module for Catalyst 6500-E, 3DES/AES at 1st year. As per best practice in network security, bidder should provide perimeter firewall product other than Cisco Make as mentioned in Annexure J, Table F, SL no. 8, 10, 11, and 12.</p>

10	Part V 5.4 Payment Terms Page 38	90% of the value of new network equipment/devices/solutions/linkimplementation/shifting/upgradation of along with Taxes, will be paid after delivery and completion of successful installation & operational, on submission of proof of delivery and the acceptance certificate duly signed by Bank's authorized official & satisfactory service report from the Bank where the systems have been installed after realizing penalty charges for late delivery & installation, if any. The balance 10% of order value will be paid after 3 months successful running.	90% of the value of new network <u>equipment/devices/solutions</u> along with Taxes, will be paid after delivery and completion of successful installation & operational, on submission of proof of delivery and the acceptance certificate duly signed by Bank's authorized official & satisfactory service report from the Bank where the systems have been installed after realizing penalty charges for late delivery & installation, if any. The balance 10% of order value will be paid after 3 months successful running.
11	Addition in Part V		<p>5.26 WARRANTY & MAINTENANCE</p> <ul style="list-style-type: none"> The Bidder shall provide warranty for all the equipment, which will be delivered & installed in sites. The period of warranty will be 36 month from the date of installation. During the warranty period the Vendor should maintain the acceptance criteria and shall be responsible for all costs relating to service, maintenance (preventive and corrective), technical support and transport charges from and to the sites in connection with the maintenance of the solution or any components/ parts there under, which, under normal and proper use and maintenance thereof, proves defective in design, material or workmanship or fails to conform to the specifications, as specified. The Vendor should inform the bank about the end of life of the product proposed. Proposed product should have warranty service as mentioned in Annexure J. Product must not be End of Life and Support in next 5 years. If offered product declared End of Life and Support within 5 years, then bidder should provide latest product with same specification or higher without any cost to the Bank. In case of damage of any equipment under AMC, bidder should replace with same equipment. In case same replacement equipment not available in market or out of sell by OEM, then bidder should replace with equivalent/higher product. <p>Bidder must have back to back support relation with the OEM's whose products are followed by the bidder to the Bank, in case the bidder is not Original Equipment Manufacturer(OEM). A commitment letter (Annexure C) from the OEM(s) has to be submitted along with the Technical bid in this regard at least for a period of 5 years for all new and support upto end of life for all product under AMC as per Annexure J & M.</p>
12	Part V 5.4 Payment against delivery of SLAs Page 40	Bank will pay charges on per site basis depending upon the achievement of uptime. However bank issues will be exempted from calculating the uptime.	Bank will pay charges <u>for equipment AMC or link management cost</u> depending upon the achievement of uptime. However bank issues will be exempted from calculating the uptime.

Uptime	% of payment	Uptime	% of payment	Uptime	% of payment
DC, DR, Treasury, ATM network		All Other site except Rural Branch		Rural Branch	
99.9% or more	100%	99.5% or more	100%	98% or more	100%
>99.7% to <=99.9%	90%	>98% to <=99.49	90%	>96% to <=97.99	90%
>99.5% to <=99.7%	80%	>97% to <=97.99	80%	>94% to <=95.99	80%
>99.3% to <=99.5%	70%	>96% to <=96.99	70%	>92% to <=93.99	70%
>99.0% to <=99.3%	60%	>95% to <=95.99	60%	>90% to <=91.99	60%
Less than 99%	Nil	Less than 95%	Nil	Less than 90%	Nil

Calculation of uptime will be monthly basis as per following criteria.

$$\frac{[\text{Total Business hours in month} - \text{Total downtime during business hours in month}] \times 100}{[\text{Total Business hours in month}]}$$

% of uptime =

$$\frac{[\text{Total Business hours in month}]}{[\text{Total Business hours in month}]}$$

Bank may monitor the links by its own tool for uptime along with Service provider. In case of difference in uptime, Bank may consider the payment based on report generated by Bank's tool, if bidder is unable to justify the difference.

Performance Measurement (SLA uptime calculation)

Working hours calculated as per the service window time for:

- A. Core & Backbone including ATM Switch & Mumbai Treasury locations will be – 24 Hrs
- B. Branch working days - 08:00 am to 08:00 pm (12 Hrs)

Total business hours for one month Case A = 24*60*30(31) = 43200 / 44640 minutes

Total business hours for one month Case B = 12*60*30(31) = 21600 / 22320 minutes

Uptime	% of payment	Uptime	% of payment	Uptime	% of payment
DC, DR		All Other branches/offices except Rural Branch		Rural Branch	
99.9% or more	100%	99.5% or more	100%	98% or more	100%
>99.7% to <=99.9%	90%	>98% to <=99.49	90%	>96% to <=97.99	90%
>99.5% to <=99.7%	80%	>97% to <=97.99	80%	>94% to <=95.99	80%
>99.3% to <=99.5%	70%	>96% to <=96.99	70%	>92% to <=93.99	70%
>99.0% to <=99.3%	60%	>95% to <=95.99	60%	>90% to <=91.99	60%
Less than 99%	Nil	Less than 95%	Nil	Less than 90%	Nil

i) In case of site is isolated due to link down the above % penalty will be deducted from the link management cost of that site. The same is applicable for the site running on secondary link due to primary link failure.

ii) In case of site is isolated due to failure of equipment at site above % of penalty will be deducted from the AMC cost of all equipment installed at of the site pro-data basis.

Calculation of uptime will be monthly basis as per following criteria.

$$\frac{[\text{Total Business hours in month} - \text{Total downtime during business hours in month}] \times 100}{[\text{Total Business hours in month}]}$$

% of uptime =

$$\frac{[\text{Total Business hours in month}]}{[\text{Total Business hours in month}]}$$

Bank may monitor the links by its own tool for uptime along with Service provider. In case of difference in uptime, Bank may consider the payment based on report generated by Bank's tool, if bidder is unable to justify the difference.

Performance Measurement (SLA uptime calculation)

Working hours calculated as per the service window time for:

		<p>E.g. If a branch down time in a particular month is 13 Hrs and Branch working is 30 days in a month, the Service Window (24Hrs) having schedule down time of 5 Hrs, then the percentage of down time calculated as</p> $= \{(43200 - 5*60) - (13*60)\} * 100 / 43200$ $= \{(42900) - (780)\} * 100 / 43200$ $= 97.5 \%$ <p>Accordingly Bank will pay 80 % on Network management service Charges of said branch.</p>	<p>A. <u>Core & Backbone locations will be – 24 Hrs</u> B. <u>Branch/offices working days -08:00 am to 08:00 pm (12 Hrs)</u></p> <p>Total business hours for one month Case A = $24*60*30(31) = 43200$ (44640) minutes</p> <p>Total business hours for one month Case B = $12*60*30(31) = 21600$ (22320) minutes</p> <p><u>E.g. If branch down time in a particular month is 10 Hrs and working is 30 days in a month, the Service Window (12Hrs) having schedule down time of 5 Hrs, then the percentage of down time calculated as</u></p> $= \{(21600 - 5*60) - (10*60)\} * 100 / (21600 - 5*60)$ $= \{(21300) - (600)\} * 100 / 21300$ $= 97.1 \%$ <p>Accordingly Bank will pay 80 % on Network management service Charges of said branch.</p>
13	Part V 5.5 Price Page 38	<p>The cost of network link must include rental charges of network equipment's e.g modem, repeater, etc. required to be terminated the link at CPE Ethernet interface. The Price Bid also must include all applicable taxes such as Sales/Service/VAT / Waybill etc. The Octroi /Entry Tax will be paid extra, wherever applicable on submission of actual Tax receipt.</p> <p>The Selected bidder is required to guarantee that exchange rate fluctuations, changes in import duty and other taxes will not affect the Rupee value of the commercial bid, over the validity period of the bid. The prospective service provider shall establish the Network and should be capable of maintaining it for a minimum period of 3 years initially and then subsequent extension for 2 years based on performance basis.</p> <p>The Bank further reserves the right to reject any or all offers based on its own evaluation of the offers received, or on the basis of stability, capabilities, track records, reputation among users and other similar features of a Selected bidder.</p> <p>Prices quoted by the selected bidder shall be in Indian Rupees, firm and not subject to any price escalation, if the order is placed within the validity period. Further, subsequent to the orders being placed/agreement executed, the selected bidder shall pass on to the Bank all fiscal benefits arising out of reductions in Government levies viz. Sales tax, excise duty, custom duty, etc.</p>	<p><u>The Price Bid also must include all applicable taxes such as Sales/Service/VAT / Waybill etc. The Octroi /Entry Tax will be paid extra, wherever applicable on submission of actual Tax receipt.</u></p> <p>The Selected bidder is required to guarantee that exchange rate fluctuations, changes in import duty and other taxes will not affect the Rupee value of the commercial bid, over the validity period of the bid. The prospective service provider shall establish the Network and should be capable of maintaining it for a minimum period of 3 years initially and then subsequent extension for 2 years based on performance basis.</p> <p>The Bank further reserves the right to reject any or all offers based on its own evaluation of the offers received, or on the basis of stability, capabilities, track records, reputation among users and other similar features of a Selected bidder.</p> <p>Prices quoted by the selected bidder shall be in Indian Rupees, firm and not subject to any price escalation, if the order is placed within the validity period. Further, subsequent to the orders being placed/agreement executed, the selected bidder shall pass on to the Bank all fiscal benefits arising out of reductions in Government levies viz. Sales tax, excise duty, custom duty, etc.</p>
14	Part V 5.21 Termination Page 47	<p>The Bank shall be entitled to terminate the agreement with the Selected bidder at any time by giving ninety (90) days prior written notice to the Selected bidder.</p> <p>The Bank shall be entitled to terminate the agreement at any time by giving notice if:</p> <ul style="list-style-type: none"> The Selected bidder breaches its obligations under the scope document or the subsequent agreement and if the breach is not cured within 30 days from the date 	<p><u>The Bank shall be entitled to terminate the agreement with the Selected bidder at any time by giving ninety (90) days prior written notice to the Selected bidder, if:</u></p> <ul style="list-style-type: none"> The Selected bidder breaches its obligations under the scope document or the subsequent agreement and if the breach is not cured within 30 days from the date of notice. The Selected bidder (i) has a winding up order made

		<p>of notice.</p> <ul style="list-style-type: none"> The Selected bidder (i) has a winding up order made against it; or (ii) has a receiver appointed over all or substantial assets; or (iii) is or becomes unable to pay its debts as they become due; or (iv) enters into any arrangement or composition with or for the benefit of its creditors; or (v) passes a resolution for its voluntary winding up or dissolution or if it is dissolved. The Selected bidder shall have right to terminate only in the event of winding up of the Bank. <p>In the event of termination of the Contract due to any cause whatsoever, [whether consequent to the stipulated term of the Contract or otherwise], UCO BANK shall be entitled to impose any such obligations and conditions and issue any clarifications as may be necessary to ensure an efficient transition and effective business continuity of the Service(s) which the selected Vendor shall be obliged to comply with and take all available steps to minimize loss resulting from that termination/breach, and further allow the next successor Vendor to take over the obligations of the erstwhile Vendor in relation to the execution/continued execution of the scope of the Contract.</p> <p>Bank shall have the right to initiate appropriate proceedings before any court of appropriate jurisdiction, should it find it expedient to do so.</p>	<p>against it; or (ii) has a receiver appointed over all or substantial assets; or (iii) is or becomes unable to pay its debts as they become due; or (iv) enters into any arrangement or composition with or for the benefit of its creditors; or (v) passes a resolution for its voluntary winding up or dissolution or if it is dissolved. The Selected bidder shall have right to terminate only in the event of winding up of the Bank.</p> <p>In the event of termination of the Contract due to any cause whatsoever, [whether consequent to the stipulated term of the Contract or otherwise], UCO BANK shall be entitled to impose any such obligations and conditions and issue any clarifications as may be necessary to ensure an efficient transition and effective business continuity of the Service(s) which the selected Vendor shall be obliged to comply with and take all available steps to minimize loss resulting from that termination/breach, and further allow the next successor Vendor to take over the obligations of the erstwhile Vendor in relation to the execution/continued execution of the scope of the Contract.</p> <p>Bank shall have the right to initiate appropriate proceedings before any court of appropriate jurisdiction, should it find it expedient to do so.</p>
15	Addition in Part V		<p>5.27 REMEDIES AND LIABILITIES</p> <p>a) The remedies in this clause are Bank's sole and exclusive remedies.</p> <p>b) Selected Bidder is hereby agrees and undertakes to the Bank that selected bidder shall remain responsible to the Bank for completion of Project as contemplated in the scope of work.</p> <p>c) If any defect/s is or are found at any stage of the Project and the Bank points out such defect(s), SELECTED BIDDER shall rectify such defect(s) to the extent and in the manner specified the scope of work.</p> <p>In the event that the SELECTED BIDDER is held liable in connection with this Master Contract, SELECTED BIDDER"s liability is limited to: -</p> <p>The Selected Bidder aggregate liability in connection with obligations undertaken as a part of the Project regardless of the form or nature of the action giving rise to such liability (whether in contract, tort or otherwise), shall be at actuals and limited to the value of the contract . The Selected Bidder liability in case of claims against the Bank resulting from Wilful Misconduct or Gross Negligence of the Selected Bidder, its employees and subcontractors or from infringement of patents, trademarks, copyrights or such other Intellectual Property Rights shall be unlimited. For breach of confidentiality the liability will be limited to the contract value with the Selected Bidder.</p> <p>„Wilful Misconduct means any act or omission on part of bidder or its agents, a. which causes harm to the Bank or is likely to cause harm to the Bank;</p> <p>or</p>

			<p>b. consequence of which may harm or are likely to cause harm to the Bank, or</p> <p>c. which adversely affects or may adversely affect the interests of the Bank, or</p> <p>d. which shows selected bidder's intention to cause harm to the Bank";</p> <p>Negligence is a disregard to an obvious risk in carrying out or execution of an obligation or duty, which has been cast upon Selected Bidder by virtue of this agreement.</p> <p>The Bank shall not be held liable for and is absolved of any responsibility or claim/litigation arising out of the use of any third party software or modules supplied by the Facility Manager as part of this scope document.</p> <p>In no event shall either party be liable for any indirect, incidental or consequential damages or indirect, incidental or consequential liability under or in connection with or arising out of this agreement or the hardware or the software delivered hereunder, howsoever such liability may arise, provided that the claims by customers, regulatory authorities users and service providers of the Bank of the agreement would be considered as a direct claim.</p> <p>Notwithstanding Clause above, in no event will SELECTED BIDDER or its affiliates, subcontractors and suppliers be liable for any of the following:</p> <p>a. Damages for loss of data, or Software restoration if it is attributable to Bank.</p> <p>b. Incidental, consequential or special damages but excluding damages for bodily injury.</p> <p>c. Damages relating to Bank's procurement of any products or services not supplied by selected bidder for the project.</p> <p>Banks right to impose Penalty for any non-adherence to the Service Level and non-performance of the obligations under the Service Level Agreement shall be in accordance with and limited as per the Service Level Agreement. Banks right to impose Liquidated Damages for any non-adherence to the timelines under the Service Level Agreement shall be in accordance with and limited as per the Service Level Agreement.</p>
16	Addition in Part V		<p>5.28 Fall Clause</p> <p>The Bidder Undertakes that it has not supplied / is not supplying identical products/systems or subsystems with same scope and terms and conditions, contracted during 6 months prior to the bid submission, at a price lower than that offered in the present the bid in respect of any other Ministry/ Department of the Government of India or PSU and if it is found at any stage that identical product or system or subsystem with same scope and terms and conditions was supplied by the BIDDER to any other Ministry/Department of Government of India or a PSU at a lower price , than that very price, with due allowance for elapsed time, will be applicable to the present case and the different in the cost would be adjusted by the BIDDER to the BANK/BUYER, if the CONTRACT has already been concluded.</p>

17	Addition in Part V		5.29 Acceptance of deliverables Service Provider will provide notice to Bank when deliverables are ready for acceptance. Acceptance of Deliverables will occur upon the date Service Provider demonstrates to Bank, by the successful completion of acceptance tests that the deliverables substantially conform to the acceptance criteria as agreed between Bank and Service Provider.
18	Annexure G Page 60 to 87	Technical Requirements Annexure G	Technical Requirements Modified Annexure G attached herewith.
19	Annexure J Page 100 to102	Technical Template Annexure J	Technical Template Modified Annexure J attached herewith
20	Annexure K Page 103 to108	Commercial Template Annexure K	Commercial Template Modified Annexure K attached herewith

Note: All other terms and conditions, clauses of the subject RFP remain unchanged. The reply to pre bid quires & changes in the RFP clause mentioned herein above will be part & parcel in the RFP.

Technical Requirements**Required Minimum Technical Features of Router- Type A Table A**

Sl. No.	Required Featured by the Bank	Yes/No
1	Hardware appliance & modular architecture for scalability and should be a single box configuration for ease of management.	
2	Should have a dedicated console port and USB port for storage of configuration/image.	
3	Should have at least 1 Nos. 10/100/1000 Mbps Ethernet interfaces.	
4	Should have at least 2 No. of 10/100/1000 Mbps Ethernet WAN Port.	
5	Routers should have at least 1 one serial interfaces for V.35	
6	Should support debugging capabilities to assist in problem resolution	
7	Should have hardware assisted VPN acceleration.	
8	Router should support minimum 10Mbps real world WAN bandwidth with all the services enabled on the router	
9	Should have other IP Services like GRE tunneling, ACLs, IPSEC VPNs, NAT services, Router should support HSRP or VRRP for redundancy	
10	Should support Firewall features (transparent and bridging).	
11	Routers should have Class-based queuing	
12	Routers should have marking, policing and shaping.	
13	Routers should support Voice traffic optimization with features like WRED, Modular QoS or equivalent and RSVP.	
14	Routers should have IPV6 compliance from day one	
15	Routers should IPv6 transport packets between IPv6-only and IPv4-only endpoints, ICMPv6, IPv6 DHCP.	
16	Support for the following IP v6 features : RIP NG , OSPF v3 , BGP Support for V6, IP V6 Dual Stack, NAT 64/NAT 64/Suitable Network address translation/tunneling for IPv6, IP v6 Policy based Routing, and IP v6 QoS, SNMP V3 over IPv6 or equivalent features.	
17	Router should support protocols like IPv4, IPv6, VRRP, Static Routes, RIPv1, RIPv2, OSPF, IS-IS, BGP, MBGP, BFD, Policy based routing, IPv4 and IPv6 tunneling from day 1	
18	The router should be capable of WAN protocols like PPP, Multilink PPP, etc.	
19	Dynamic Host Control Protocol (DHCP) server/relay/client	
20	Dynamic DNS Support	
21	Support for 802.1q VLANs, Demilitarized Zone (DMZ)	
22	Should have IGMP v1/v2/v3, PIM-DM, PIMSM, Source Specific Multicast (SSM)	
23	Routers should have Configuration rollback	
24	Should support network traffic accounting, usage-based network billing, network planning, security, Denial of Service (DoS) monitoring capabilities and network monitoring.	
25	Should have extensive support for SLA monitoring for metrics like delay, latency, jitter, packet loss, RTP-Based VoIP traffic, CRTP..	
26	Routers should support Software upgrades as and when necessary	
27	Routers should have SNMPv2 and SNMPv3	
28	Routers should have AAA authentication using RADIUS and TACACS	
29	Routers should have Packet Filters like: Standard ACL, Extended ACL, Time range ACL"s etc.	
30	Router should support advanced application inspection and control	
31	Routers should have Tunnels (GRE, IPsec)	
32	The router should support IPsec Framework for Secured Data transfer Key Exchange : Internet Key Exchange (IKE), IKEv2, Pre-Shared Keys (PSK), Public Key Infrastructure PKI (X.509), RSA encrypted nonces/ RSA Signatures etc, IPsec Data Encapsulation AH and ESP or equivalent function.	
33	NAT transparency, Firewall support for clients	
34	IPsec 3DES termination/initiation, IPsec passthrough	
35	Routers should have DES, 3DES, AES (256 bit) encryption, Authentication Algorithm: SHA1 and SHA2, Group: Diffie-Hellman (DH) Group 1, 2, 5	
36	Routers should have generation of SNMP traps and syslog	
37	Routers should have Network address translation (NAT) and PAT	
38	Extensive debugs on all protocols	
39	Shall have Secure Shell for secure connectivity	
40	Should have out of band management through console and an external modem for remote management	
41	Management should support : Telnet, Simple Network Management Protocol (SNMP), CLI/Web based HTTP management, RADIUS	
42	Attach solution document containing detailed bill of material (make, model, OS details:	

	version, date of release, date of release of next version, end of sale & support date, product development path, etc.)	
43	Solution/device should integrate seamlessly with Bank's existing network Infrastructure.	

Required Minimum Technical Features of Router- Type B Table B

Sl. No.	Required Featured by the Bank	Yes/No
1	Hardware appliance & modular architecture for scalability and should be a single box configuration for ease of management.	
2	Should have a dedicated console port and USB port for storage of configuration/image.	
3	Should have at least 2 Nos. 10/100/1000 Mbps Ethernet interfaces.	
4	Should have at least 2 No. of 10/100/1000 Mbps Ethernet WAN Port.	
5	Routers should have at least 1 open slots for V.35 serial interfaces	
6	Should support debugging capabilities to assist in problem resolution	
7	Should have hardware assisted VPN acceleration.	
8	Router should support minimum 50 Mbps real world WAN bandwidth with all the services enabled on the router	
9	Should have other IP Services like GRE tunneling, ACLs, IPSEC VPNs, NAT services, Router should support HSRP or VRRP for redundancy	
10	Should support Firewall features (transparent and bridging).	
11	Routers should have Class-based queuing	
12	Routers should have marking, policing and shaping.	
13	Routers should support Voice traffic optimization with features like WRED, Modular QoS or equivalent and RSVP.	
14	Routers should have IPV6 compliance from day one	
15	Routers should IPv6 transport packets between IPv6-only and IPv4-only endpoints, ICMPv6, IPv6 DHCP.	
16	Support for the following IP v6 features : RIP NG , OSPF v3 , BGP Support for V6, IP V6 Dual Stack, NAT 64/NAT 64/Suitable Network address translation/tunneling for IPv6, IP v6 Policy based Routing, and IP v6 QoS, SNMP V3 over IPv6 or equivalent features.	
17	Router should support protocols like IPv4, IPv6, VRRP, Static Routes, RIPv1, RIPv2, OSPF, IS-IS, BGP, MBGP, BFD, Policy based routing, IPv4 and IPv6 tunneling from day 1	
18	The router should be capable of WAN protocols like PPP, Multilink PPP, etc.	
19	Dynamic Host Control Protocol (DHCP) server/relay/client	
20	Dynamic DNS Support	
21	Support for 802.1q VLANs, Demilitarized Zone (DMZ)	
22	Should have IGMP v1/v2/v3, PIM-DM, PIMSM, Source Specific Multicast (SSM)	
23	Routers should have Configuration rollback	
24	Should support network traffic accounting, usage-based network billing, network planning, security, Denial of Service (DoS) monitoring capabilities and network monitoring.	
25	Should have extensive support for SLA monitoring for metrics like delay, latency, jitter, packet loss, RTP-Based VoIP traffic, CRTP..	
26	Routers should support Software upgrades as and when necessary	
27	Routers should have SNMPv2 and SNMPv3	
28	Routers should have AAA authentication using RADIUS and TACACS	
29	Routers should have Packet Filters like: Standard ACL, Extended ACL, Time range ACL's etc.	
30	Router should support advanced application inspection and control	
31	Routers should have Tunnels (GRE, IPSec)	
32	The router should support IPSec Framework for Secured Data transfer Key Exchange : Internet Key Exchange (IKE), IKEv2, Pre-Shared Keys (PSK), Public Key Infrastructure PKI (X.509), RSA encrypted nonces/ RSA Signatures etc, IPSec Data Encapsulation AH and ESP or equivalent function.	
33	NAT transparency, Firewall support for clients	
34	IPSec 3DES termination/initiation, IPSec passthrough	
35	Routers should have DES, 3DES, AES (256 bit) encryption, Authentication Algorithm: SHA1 and SHA2, Group: Diffie-Hellman (DH) Group 1, 2, 5	
36	Routers should have generation of SNMP traps and syslog	
37	Routers should have Network address translation (NAT) and PAT	
38	Extensive debugs on all protocols	
39	Shall have Secure Shell for secure connectivity	
40	Should have out of band management through console and an external modem for remote management	
41	Management should support : Telnet, Simple Network Management Protocol (SNMP), CLI/Web based HTTP management, RADIUS	

42	Attach solution document containing detailed bill of material (make, model, OS details: version, date of release, date of release of next version, end of sale & support date, product development path, etc.)	
43	Solution/device should integrate seamlessly with Bank's existing network infrastructure.	

Required Minimum Technical Features of Router- Type C Table C

Sl. No.	Required Feature by the Bank	Yes/No
1	Chassis based & modular architecture for scalability and should be a single box configuration for ease of management.	
2	Should have a dedicated console port and USB port for storage of configuration/image.	
3	Should have at least 3 Nos. 10/100/1000 Mbps Ethernet interfaces.	
4	Should have at least 2 No. of 10/100/1000 Mbps Ethernet WAN Port.	
5	Routers should have at least 2 open slot for modular LAN and WAN connectivity options including Gigabit Ethernet and Fast Ethernet, T1/E1, V.35/G.703 Serial, 3G Wireless(Both HSPA and CDMA/WCDMA) interface modules.	
6	Should support debugging capabilities to assist in problem resolution	
7	Should have hardware assisted VPN acceleration.	
8	Router should support minimum 300 Mbps real world WAN bandwidth with all the services enabled on the router	
9	Should have other IP Services like GRE tunneling, ACLs, IPSEC VPNs, NAT services, Router should support HSRP or VRRP for redundancy	
10	Should support Firewall features (transparent and bridging).	
11	Routers should have Class-based queuing	
12	Routers should have marking, policing and shaping.	
13	Routers should support Voice traffic optimization with features like WRED, Modular QoS or equivalent and RSVP.	
14	Routers should have IPV6 compliance from day one	
15	Routers should support IPv6 transport packets between IPv6-only and IPv4-only endpoints, ICMPv6, IPv6 DHCP.	
16	Support for the following IP v6 features : RIP NG , OSPF v3 , BGP Support for V6, IP V6 Dual Stack, NAT 64/NAT 64/Suitable Network address translation/tunneling for IPv6, IP v6 Policy based Routing, and IP v6 QoS, SNMP V3 over IPv6 or equivalent features.	
17	Router should support protocols like IPv4, IPv6, VRRP, Static Routes, RIPv1, RIPv2, OSPF, IS-IS, BGP, MBGP, BFD, Policy based routing, IPv4 and IPv6 tunneling from day 1	
18	The router should be capable of WAN protocols like PPP, Multilink PPP, etc.	
19	Dynamic Host Control Protocol (DHCP) server/relay/client	
20	Dynamic DNS Support	
21	Support for 802.1q VLANs, Demilitarized Zone (DMZ)	
22	Should have IGMP v1/v2/v3, PIM-DM, PIMSM, Source Specific Multicast (SSM)	
23	Routers should have Configuration rollback	
24	Should support network traffic accounting, usage-based network billing, network planning, security, Denial of Service (DoS) monitoring capabilities and network monitoring.	
25	Should have extensive support for SLA monitoring for metrics like delay, latency, jitter, packet loss, RTP-Based VoIP traffic, CRTP..	
26	Routers should support Software upgrades as and when necessary	
27	Routers should have SNMPv2 and SNMPv3	
28	Routers should have AAA authentication using RADIUS and TACACS	
29	Routers should have Packet Filters like: Standard ACL, Extended ACL, Time range ACL's etc.	
30	Router should support advanced application inspection and control	
31	Routers should have Tunnels (GRE, IPSec)	
32	The router should support IPSec Framework for Secured Data transfer Key Exchange : Internet Key Exchange (IKE), IKEv2, Pre-Shared Keys (PSK), Public Key Infrastructure PKI (X.509), RSA encrypted nonces/ RSA Signatures etc, IPSec Data Encapsulation AH and ESP or equivalent function.	
33	NAT transparency, Firewall support for clients	
34	IPSec 3DES termination/initiation, IPSec passthrough	
35	Routers should have DES, 3DES, AES (256 bit) encryption, Authentication Algorithm: SHA1 and SHA2, Group: Diffie-Hellman (DH) Group 1, 2, 5	
36	Routers should have generation of SNMP traps and syslog	
37	Routers should have Network address translation (NAT) and PAT	
38	Extensive debugs on all protocols	
39	Should have Secure Shell for secure connectivity	
40	Should have out of band management through console and an external modem for remote	

	management	
41	Management should support : Telnet, Simple Network Management Protocol (SNMP), CLI/Web based HTTP management, RADIUS.	
42	Attach solution document containing detailed bill of material (make, model, OS details: version, date of release, date of release of next version, end of sale & support date, product development path, etc.)	
43	Solution/device should integrate seamlessly with Bank's existing network Infrastructure.	

Required Minimum Technical Features of Switch Type A Table D

Sl. No.	Required Featured by the Bank	Yes/No
1	Should be a single box configuration for ease of management.	
2	Switch should have minimum 50 Gbps Switching capacity all the services enabled on switch.	
3	Switch should support VCS or VSS or equivalent architecture by which two separate switches can be combined in a single switch fabric and managed as single switch.	
4	Switch should support IPv4 and IPv6 switching and routing in hardware from day 1.	
5	Switch should have minimum 24 10/100/1000 Mbps Ethernet port, 2 1G SFP Port.	
6	IEEE 802.1Q VLAN encapsulation. Upto 64 VLANs should be supported. Support for 4000 VLAN IDs. Centralized VLAN Management. VLANs created on the Core Switches should be propagated automatically. Should support 802.1d, 802.1s, 802.1w, 802.3ad, Port Aggregation Protocol (PAgP), Link Aggregation Protocol (LACP). Support for Detection of Unidirectional Links and to disable them to avoid, Per-port broadcast, multicast, and storm control to prevent faulty end stations from degrading overall systems performance.	
7	Support for minimum 200 MAC addresses	
8	Should support Private VLAN , VLAN Aggregation , Translation and 802.1v	
9	Must support Layer2 Ping and Layer 2 Traceroute for connectivity and Fault Management Must support multicast Traceroute.	
10	Should support SNMP and syslog Notification for MAC addition, deletion and movement across ports	
11	Support for IP Unicast routing protocols (static, RIP v1 & v2, OSPF & Policy based routing)	
12	Should support DHCP	
13	Should have out of band management through console and an external modem for remote management	
14	Management should support : Telnet, Simple Network Management Protocol (SNMP), CLI/Web based HTTP management, RADIUS	
15	Attach solution document containing detailed bill of material (make, model, OS details: version, date of release, date of release of next version, end of sale & support date, product development path, etc.)	
16	Solution should integrate seamlessly with Bank's existing network Infrastructure.	

Required Minimum Technical Features of Switch Type B Table E

Sl. No.	Required Featured by the Bank	Yes/No
1	Should be a single box configuration for ease of management.	
2	Switch should have minimum 50 Gbps Switching capacity all the services enabled on switch	
3	Switch should support IPv4 and IPv6 switching in hardware from day 1.	
4	Switch should have minimum 24 10/100/1000 Mbps Ethernet port	
5	IEEE 802.1Q VLAN encapsulation. Upto 64 VLANs should be supported. Support for 4000 VLAN IDs. Centralized VLAN Management. VLANs created on the Core Switches should be propagated automatically. Should support 802.1d, 802.1s, 802.1w, 802.3ad, Port Aggregation Protocol (PAgP), Link Aggregation Protocol (LACP). Support for Detection of Unidirectional Links and to disable them to avoid, Per-port broadcast, multicast, and storm control to prevent faulty end stations from degrading overall systems performance..	
6	Support for minimum 200 MAC addresses	
7	Should support Private VLAN , VLAN Aggregation , Translation and 802.1v	
8	Must support Layer2 Ping and Layer 2 Traceroute for connectivity and Fault Management Must support multicast Traceroute.	
9	Should support SNMP and syslog Notification for MAC addition, deletion and movement across ports	
10	Should have out of band management through console and an external modem for remote management	
11	Management should support : Telnet, Simple Network Management Protocol (SNMP), CLI/Web based HTTP management, RADIUS	
12	Attach solution document containing detailed bill of material (make, model, OS details: version, date of release, date of release of next version, end of sale & support date, product	

	development path, etc.)	
13	Solution should integrate seamlessly with Bank's existing network Infrastructure.	

Required Minimum Technical Features of Firewall Table F

Sl. No.	Required Featured by the Bank	Yes/No
1	Chassis based & modular architecture for scalability	
2	Firewall should have at least 6 no. of GE ports	
3	The appliance should be capable of providing Firewall, VPN Services and Next Generation Firewall feature. 300 remote VPN license required with 1 pare of Firewall.	
4	The platform should support VLAN tagging (IEEE 802.1q)	
5	Should have a 64Bit Multi-Core Processor and should not be ASIC based architecture.	
6	The platform shall have dedicated interface for out-of bound management	
7	The Firewall should support CA functionality	
8	Support for minimum 1000 MAC addresses	
9	Firewall performance should be minimum real world throughput 20 Gbps after enabling all function like IPS, QoS, and malware protection.	
10	Firewall should be capable configuring Policies using Command Line (CLI) as a last resort in case of Emergency.	
11	Firewall should support minimum 500,0000 concurrent connections	
14	Firewall should support minimum 100000 new conections per second (cps)	
15	deliver VPN throughput minimum 300 Mbps	
16	Should support grouping of physical interfaces withing and across Fixed and Expansion ports into one single physical or logical interface	
17	Firewall should support memory atleast 8 GB Memory for better and faster processing.	
18	Should be open architecture based on multi-core cpu's to protect & scale against dynamic latest security threats.	
19	The firewall shall be deployed in high availability mode (hot stand-by redundancy), have fault tolerance and shall provide stateful failover	
20	The firewall shall have a powerful OS that is hardened and is based upon minimal feature sets.	
21	There shall be support for traffic based and user based access control.	
22	The broad default policy for the firewall for handling inbound traffic shall be to block all packets and connections unless the traffic type and connections have been specifically permitted	
23	It shall support SNMP (Simple Network Management Protocol) v 2.0 and v 3.0.	
24	Firewall should support Single Sign On (SSO)	
25	Should support translating between IPv4 and IPv6 for the following inspections: DNS, FTP,ICMP,HTTP	
26	Network address translation (NAT) shall be supported so that the private IP addresses of hosts and the structure of an internal network can be concealed by the firewall.	
27	Network Address Translation (NAT) shall be configurable as 1:1, 1: many, many: 1, many: many, flexible NAT (overlapping IPs). Reverse NAT shall be supported.	
28	Port address translation/Masquerading shall be provided for	
29	Dynamic Host Configuration Protocol (DHCP) over Virtual Private Network (VPN) shall be supported for dynamic allocation of IP addresses.	
30	The firewall shall support a number of routing options and configurations. Routing protocol support shall include static routes, Open Shortest Path First (OSPF), RIPv1/v2 etc.	
31	Virtual LAN (VLAN) support, high port density, WAN support and expandability of interfaces over time are some important network integration features shall be supported.	
32	The firewall IP stack shall be IPv6 ready.	
33	The firewall shall mask the internal network from the external world.	
34	The firewall shall provide robust access control capability and be fast in making access control decisions. Access Control shall be done based on criteria such as source, destination IPs, port number, protocol, traffic type, application, date information (day of week, time of day), etc.	
35	Multi-layer, stateful, applicationbased filtering shall be done	
36	It shall provide network segmentation features with powerful capabilities that facilitate deploying security for various internal, external and DMZ (Demilitarized Zone) sub-groups on the network, to prevent unauthorized access	
37	There shall be support for detection of reconnaissance attempts such as IP address sweep, port scanning etc.	
38	Firewall itself shall be resistant to attack and shall have protection against firewall evasion	

	techniques.	
39	Some basic attack protection features listed below but not limited to : Maximum no of protections against attacks that exploit weaknesses in the TCP/IP protocol suite It shall enable rapid detection of network attacks TCP reassembly for fragmented packet protection Brute force attack mitigation. SYN cookie protection , SYN Flood, Half Open Connections and NUL Packets Protection against IP spoofing Malformed packet protection Java blocking, and real-time alerts	
40	Full H.323v1-5 (Firewall Traversal), SIP (Session Initiation Protocol), gatekeeper support, outbound bandwidth management, full interoperability with common and popular VoIP/VC gateway and communications devices shall be supported, apart from supporting all protocols.	
41	The firewall shall support Internet Protocol Security (IPSec) & SSL	
42	Key exchange with latest Internet Key Exchange (IKE), IKEv2, Public Key Infrastructure PKI (X.509) shall be catered to.	
43	Site-to-site VPN tunnels: full-mesh / star topology shall be supported.	
44	Support Latest Encryption algorithms including AES 128/192/256(Advanced Encryption Standards), 3DES(Data Encryption Standard) etc.	
45	Support Latest Authentication algorithms including SHA-1(Secure Hash Algorithm-1), SHA-2(Secure Hash Algorithm-2) etc.,	
46	IPSec NAT traversal shall be supported.	
47	VPN supporting atleast 300 IPSec / SSL VPN peers	
48	The solution should support the following File/Media Types for Malware identification: PDF, ZIP, 7Z, RAR, CAB, PKZIP, EXE, DLL, SYS, SCR, CPL, OCX, Java, Flash, MS office files.	
49	The solution should support down selection and only analyzes files deemed suspicious.	
50	The solution should have the ability to heuristically detect and decode the presence of shell code	
51	The solution should have the ability to detect and scan pdf files for embedded code	
52	The solution should have capability to fully reveal malware's current and potential payloads or equivalent features.	
53	The solution should provide detection, analysis and repair capability against malware-based attacks	
54	The solution should provide a detailed list of every DLL and API referenced, all header information about the binary, and complete assembly-language listing of the binary code or equivalent features.	
55	The solution should provide reports to shows all the activities the malware code performs related to file systems, Windows registry, network operations, Processes and any other miscellaneous operations	
56	The solution should provide summary for instance, whether the malware wrote into a certain file, modified a registry setting, opened a port or communicated to a specific url, or changed the name of a running process to hide itself or equivalent features.	
57	The solution should identify any logic bombs (time based execution delays) hidden in the malware waiting for a trigger to cause damage at a later time	
58	The solution should provide the ability to upload gold image and analyze threats under conditions of actual host environment.	
59	Solution should provide Detailed Technical Report, Behavior Summary Report and a Logic Execution Path Map.	
60	The solution should recognize new variants of existing malware families and identify new families.	
61	The Solution should support the following multiple advanced malware analysis methods:	
62	Solution should provide high Threat protection rate minimum of 99%.	
63	The solution shall give CVE number for the Intrusion events detected and shall capture packet for each intrusion event	
64	The solution should automatically map event to the IP, Geography information, to the user, system affected	
65	The solution must be capable of significantly reducing operator effort and accelerating response to threats by automatically prioritizing alerts, ideally based on the potential for correlated threats to successfully impact the specific hosts they are directed toward.	
66	The IPS detection methodologies shall consist of Signature based detection using real time updated database & Anomaly based detection that is based on thresholds	
67	The proposed system shall support One-arm IDS (sniffer mode)	
68	The device shall allow administrators to create Custom IPS signatures	
69	Consists of vendor's original threat intelligence and is not overly dependent on information available in the public domain.	

70	Is continuously updated with new threat intelligence, including detailed help text, in an automated fashion and without physical access to the unit.	
71	Security information is meaningful, comprehensive and freely available to customers and non-customers via a publicly accessible database.	
71	Detects and blocks all known, high risk exploits along with their underlying vulnerability (not just one exploit of that vulnerability).	
73	Allows users to control the number of times a sensor notifies the console when a flood type attack occurs. For example, the sensor must be configurable to send a single alert every five minutes vs. sending an alert for every single packet associated with the attack. This will avoid overwhelming the console and the internal network with alerts.	
74	Must be capable of performing packet-level forensics and capturing raw packet data in response to individual events	
75	The detection engine must support multiple options for directly responding to events, such as monitor only, block offending traffic, replace packet payload, and capture packets	
76	The solution must be capable of passively gathering information about session flows for all monitored hosts, including start/end time, ports, services, and amount of data.	
77	Accurately detects intrusion attempts and discerns between the various types and risk levels including unauthorized access attempts, pre-attack probes, suspicious activity, DoS, DDoS, vulnerability exploitation, brute force, hybrids, and zero-day attacks.	
78	Detection rules must be based on an extensible, open language (API) that enables users to create their own rules, as well as to customize any vendor-provided rules.	
79	Detection rules provided by the vendor must be documented, with full descriptions of the identity, nature, and severity of the associated vulnerabilities and threats being protected against.	
80	The detection engine must be capable of detecting and preventing a wide variety of threats (e.g., malware, network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, zero -day threats, etc.)which require license for cloud sandboxing feature with hash only	
81	The detection engine must incorporate multiple approaches for detecting threats, including at a minimum exploit -based signatures, vulnerability -based rules, protocol anomaly detection, and behavioral anomaly detection techniques. Identify and explain each type of detection mechanism supported.	
82	The detection engine must inspect not only Network Layer details and information resident in packet headers, but a broad range of protocols across all layers of the computing stack and packet payloads as well.	
83	The detection engine must be resistant to various URL obfuscation techniques common to HTML -based attacks	
84	The solution must be capable of detecting and blocking IPv6 attack	
85	The solution must provide IP reputation feed that comprised of several regularly updated collections of IP addresses determined by the proposed security vendor to have a poor reputation.	
86	The solution should be capable of providing network -based detection of malware by checking the disposition of known files in the cloud using the SHA -256 file -hash as they transit the network (SHA -256 and target IP address should be given to aid remediation efforts) with enabling justadvance malware license if require in near future	
87	The solution must be capable of passively gathering information about network hosts and their activities, such as operating system, services, open ports, client applications, and vulnerabilities, to assist with multiple activities, such as intrusion event data correlation, elimination of false positives, and policy compliance.	
88	The solution must be capable of passively gathering information about session flows for all monitored hosts, including start/end time, ports, services, and amount of data.	
89	The solution must be capable of storing user -defined host attributes, such as host criticality or administrator contact information, to assist with compliance monitoring.	
90	The solution must be capable of passively gathering user identity information, mapping IP addresses to username, and making this information available for event management purposes.	
91	The solution must be capable of passively gathering details unique to mobile devices traffic to identify a wide variety of mobile operating systems, mobile applications and associated mobile device hardware.	
92	The solution must provide a detailed, interactive graphical summary that includes data on applications, application statistics, connections, intrusions events, hosts, servers, users, file -types, malwares and relevant URLs. These data should be presented by detailed lists (Administrator should easily create and apply custom filters to fine -tune the analysis).	

93	Appliance have capacity to block source based on geo -location	
94	The solution must be capable of employing an extensive set of contextual information (e.g., pertaining to the composition, configuration, and behavior of the network and its hosts) to improve the efficiency and accuracy of both manual and automatic analysis of detected events.	
96	The solution must be capable of dynamically tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.) with minimal human intervention.	
97	Should have identification support for atleast 3000 applications and the identification should be regardless of ports. The application needs to be predefined on the box.	
98	The proposed system shall have the ability to identify, block the following common P2P applications : Gnutella (Napshare, iMesh, Mldonkey, morph, Xolox, BearShare, FOXY), Bittorrent, Kaaza, WinY, edonkey).	
99	The solution must integrate application control to reduce risks associated with applications usage and client -side attacks. It should provide a means of enforcing acceptable use policies of up to 3000 application detectors.	
100	The solution must support creation of user -defined application protocol detectors.	
101	The solution must have content awareness with comprehensive file detection policies and blocking of files by types, protocols and directions.	
102	The proposed solution should provide an option to include URL filtering for enforcing Internet content filtering so as to reduce web born threats and improve productivity.	
103	Each URL in the data set must has an associated category and reputation. URL category is a general classification for the URL while URL reputation represents how likely the URL is to be used for purposes that might be against the organization's security policy.	
104	The solution must be capable of easily identifying all hosts that exhibit a specific attribute or non - compliance condition.	
110	The management platform must be capable of centralized, life cycle management for all NGFW services/devices.	
111	The management platform must be delivered in virtual appliance form factor (management system and UI must provide the same features and functions as in the physical appliance).	
112	The management platform must be capable of aggregating IDS/IPS events and centralized, real-time monitoring and forensic analysis of detected events.	
113	The management platform must be accessible via a web-based interface/ client software.	
114	The management platform must provide a highly customizable dashboard.	
115	The management platform must be capable of integrating third party vulnerability information into threat policy adjustment routines and automated tuning workflows.	
116	The management platform must be capable of role-based administration, enabling different sets of views and configuration capabilities for different administrators subsequent to their authentication.	
117	The management platform must include a scheduling subsystem to facilitate automation of routine tasks, such as backups, upgrades, report creation, and policy application.	
118	The management platform must include one or more default (i.e., pre-defined) detection policy configurations to help simplify initial deployment.	
119	The management platform must provide the capability to easily view, enable, disable, and modify individual rules, as well as groups or categories of rules.	
120	The management platform must be capable of automatically receiving rule updates published by the vendor and automatically distributing and applying those rule updates to sensors.	
121	The management platform must be capable of backup and rollback for sensor configurations and the management platform itself.	
123	The management platform must provide the ability to view the corresponding detection rule for each detected event, along with the specific packet(s) that caused it to be triggered.	
124	The management platform must support both internal and external databases/systems for storage of event data, logs, and other systemgenerated information..	
125	The management platform must be capable of synchronizing time between all components of the system via NTP.	
126	The management platform must be capable of logging all administrator activities, both locally and to a remote log server.	
127	The solution must support LDAP for single sign-on to sensors and the management console.	
128	The management platform must provide robust reporting capabilities, including a selection of pre-defined reports and the ability for complete customization and generation of new reports.	
129	The reporting tool needs to be bundled or quoted along with the solution.The logging and analysis should either be an appliance or on a dedicated PC/ Server platform. The bidder should take the responsibility of supplying the hardware and the OS with suitable warranty.	

130	The management platform must allow quick report customization by importing from dashboards, workflows and statistics summaries.	
131	The management platform must provide multiple report output types or formats, such as PDF, HTML, and CSV.	
132	The management platform must support multiple mechanisms for issuing alerts (e.g., SNMP, e-mail, SYSLOG).	
133	Firewall should able to handle all ATM, NPCI, Payment gateway traffic at existing Bank's Network.	
134	Attach solution document containing detailed bill of material (make, model, OS details: version, date of release, date of release of next version, end of sale & support date, product development path, etc.)	
135	Solution should integrate seamlessly with Bank's existing network Infrastructure.	

Required Minimum Technical Features of IPS Table G

Sl. No.	Required Featured by the Bank	Yes/No
1	IPS should The appliance should be rack mountable and support side rails if required or inbuilt in proposed Firewall as per above Table F. Bidder may supply & installed Firewall with inbuilt IPS in same appliance without any performance issue and should comply all technical requirement of Firewall & IPS as per Annexure F & G	
2	Proposed Intrusion Prevention System should have at least 4x10/100/1000 interfaces	
3	IPS device should have console port and USB Ports	
4	Proposed IPS if, appliance should be supplied with minimum of 16 GB RAM	
5	The proposed device should have Intrusion prevention sensors delivering a minimum of 10 Gbps of context-aware , real-world traffic inspection (enabling all functions)	
6	IPS device should perform stateful pattern recognition to identify vulnerability-based attacks through the use of multi-packet inspection across all protocols.	
7	The proposed IPS must perform protocol decoding and validation for network traffic including: IP, TCP, UDP, and ICMP.	
8	IPS should provide anomaly identification for attacks that may cover multiple sessions and connections, using techniques based on identifying changes in normal network traffic patterns	
9	Should support creation of baseline of normal network traffic and then uses baseline to detect worm-infected hosts	
10	Should support creation of baseline of normal network traffic and then uses baseline to detect worm-infected hosts	
11	Must be able to identify Layer 2 Address Resolution Protocol (ARP) attacks and man-in-the-middle attacks	
14	The sensors should be able to detect attacks running inside of these tunneling protocols such as GRE, IP-in-IP, MPLS, and IPv4/IPv6.	
15	The IPS should be able to inspect SSL/https traffic	
16	Can exceptions be setup to filter out, fine-tune or adjust the actions for specific attacker or destination IP on a per signature basis	
17	The proposed product should be resistant to IPS evasion and protection from anti-NIPS (Network Intrusion Prevention System) techniques.	
18	Proposed IPS should support a minimum of average inspection throughput of 10 Gbps	
19	The average latency of the proposed IPS should be less than 150 microseconds	
20	IPS must support a minimum of 5 million concurrent connections.	
21	Support more than 1, 00,000 new sessions per second processing	
22	Proposed solution should have automatic bypass for IPS in case of performance suffer beyond defined administrative threshold or IPS function/engine fails	
23	IPS should have the functionality of Software Fail Open.	
24	IPS Software Fail Open functionality can be defined in terms Gateway Threshold of Memory or CPU and should have an option to trigger the mail if required.	
25	The IPS should support Active/Active and Active/ Standby High Availability feature.	
26	Proposed IPS solution must be capable to detect device failure, link and path failure	
27	IPS appliance failover should be complete stateful in nature without any manual intervention	
28	Proposed IPS solution should support Vulnerability and Exploit signatures, Protocol validation, Anomaly detection, Behaviour-based detection and reputation based filtering	
29	IPS profile can be defined to Deactivate protections with Severity, Confidence level, Performance impact, Protocol Anomalies	
30	IPS Profile should have an option to select or re-select specific signatures that can be	

	deactivated	
31	Intrusion Prevention should have the option to add exceptions for network and services.	
32	IPS should provide rate shaping to prioritize known, normal traffic flows and unknown traffic flows	
33	IPS Policy to Block the traffic by country should have an option to configure in incoming direction, Outgoing direction or both.	
34	IPS events/protection exclusion rules should be created and the packet data should be viewed directly from log entries.	
35	Application Intelligence should have controls for Instant Messenger, Peer-to-Peer, Malware Traffic etc.	
36	Instant Messenger should have options to Block File Transfer, Block Audio, Block Video, Application Sharing and Remote Assistance	
37	The proposed IPS should have an option to create your own signatures with an open signature language	
38	IPS should provide detailed information on each protection, including: Vulnerability and threat descriptions, Threat severity, Performance impact, Release date, Industry Reference, Confidence level etc.	
39	Proposed IPS must have an embedded GUI Based Management interface.	
40	Proposed IPS should have the options of policy configuration, event management, health management and reporting.	
41	IPS device should have features to prioritize and send alerts to users after an alert action is taken place	
42	Proposed IPS should be constantly updated with new defences against emerging threats.	
43	IPS updates should have an option of Automatic downloads and scheduled updates so that it can be scheduled for specific days and time	
44	Should have flexibility to define newly downloaded protections will be set in Detect or Prevent mode.	
45	Activation of new protections based on parameters like Performance impact, Confidence index, Threat severity etc	
46	Attach solution document containing detailed bill of material (make, model, OS details: version, date of release, date of release of next version, end of sale & support date, product development path, etc.)	
47	Solution should integrate seamlessly with Bank's existing network Infrastructure.	

Required Minimum Technical Features of WAN Optimization Table H

Sl. No.	Required Featured by the Bank	Yes/No
1	The WAN Optimization device should be based on dedicated Appliance. Rack mounting kit should be supplied along with the appliance	
2	Should have minimum 4 x 10/100/1000 Base-T Ports for inline deployment with fail-to-wire capability. In total 6 ports are required from day one	
3	Should support optimization for minimum of 10,000 concurrent TCP connections from day one, with scalability option when configured in full transparency mode. Further Bidder shall ensure that there is no application performance issue and should compress all types of application traffic i.e. Finacle, ATM, Mail Messaging (Exchange 2010), WEB Portal, etc. originating from Branch/office locations till Primary Data Center, Bangalore and Disaster Recovery Site, Kolkata. The WAN Optimization solution is being procured for 4 international Branches.	
4	Should support a minimum compressed throughput (WAN throughput) of 1000 Mbps from day one	
5	Should have 48 GB RAM from day one. During the contract period the Bidder shall ensure that there is no performance issue because of memory requirement. Incase any such issues are observed the Bidder shall provide additional memory and Bank shall not pay for the same	
6	Should have Redundant Power Supply.	
7	Should support Transport flow TCP optimization to improve application packet flow under unfavorable WAN Condition such as packet loss and small initial windows. Should support any TCP based applications	
8	Should support advance network compression that uses a bidirectional database to store previously seen TCP traffic and replace redundant patterns with very small signatures.	
9	Should support re-transmission of lost Data in case of packet-loss.	
10	The Caching Architecture should be flexible to accommodate and prioritize next generation applications like VDI, Video, HTTP etc .	

11	Should allow to configure Bidirectional Caching i.e. caching in DC end Appliance & Branch end Appliance for specific protocols like FTP, HTTP, Email etc	
12	Single instance store - Solution should support single universal dictionary for maintaining larger histories without requiring per peer data store. Architecture of the solution must ensure that single copy of any content is maintained irrespective of the peer is being sent to	
13	Content aware de-duplication: The solution must provide Content Aware De-Duplication with ability to distinguish protocol & applications. At the same time it must preserve TCP/IP information like Source & Destination IP Address, Source Port & Destination port & DSCP marking while optimizing the traffic	
14	Should support compression with a connection oriented compression history to further reduce the amount of bandwidth consumed by a TCP connection	
15	Should support integration with network management and monitoring systems.	
16	The WAN Optimization solution should be transparent to NetFlow export on the router or intermediary devices.	
17	Should support peering along with presence in management domain for up to minimum of 500 branches with WAN optimization devices.	
18	The Solution should support advance optimization for CIFS protocol including following features;- Safe data & Meta Data Caching for higher optimization and data coherency; Read-ahead & message Pipelining to mitigate send-and-wait behavior of CIFS	
19	The Solution should support MAPI Acceleration to improve email delivery, calendaring, contacts access over WAN. It should have following features	
20	Advance Email Compression & Object delivery acceleration	
21	Should provide optimization transparently requiring no change to existing infrastructure.	
22	The solution should provide HTTP & HTTPS Acceleration with following features;- Should support "Pre-Cache Acceleration" (PCA) which helps speed up the rendering of Web pages by eliminating repetitive trips over the WAN connection to validate the freshness of content. client's browser must query the remote server with an HTTP 304 request for the "freshness value" of the object	
23	Should support TCP optimization for efficient data transfer across WAN, higher bandwidth utilization, faster recovery after any packet loss. TCP optimization must include Windows Scaling, Slow start with congestion avoidance, Fast Convergence & Selective acknowledgements to ensure efficient throughput in Long FAT Networks	
24	Should support local response based on cached metadata from previously seen server responses & Server Compression.	
25	The solution should preserve trust boundaries by not distribute private keys beyond the data center device while optimizing SSL/HTTPS traffic	
26	All certificates and private keys should be stored securely on the Data Center Devices	
27	HTTPs acceleration: Support for HTTPS application acceleration blueprint to address protocol chattiness and performance issues. Solution must able to intercept the HTTPS traffic for content deduplication and protocol optimization.	
28	The solution must support acceleration for Server Message Block Version 2 (SMBv2) and signed SMBv2 protocols.	
29	The Solution should support NFS Acceleration with Metadata optimization, Read-ahead optimization, File write optimization etc	
30	Should integrate with existing network devices like router & firewalls transparently	
31	Should preserve network information like Source IP, Destination IP, Source Port, Destination Port, QOS marking throughout the network.	
32	Should support following deployment model to suite any Branch environment Inline Deployment with fail to wire functionality WCCP V2 redirection with Routers & Switches or equivalent Policy Based Redirection (PBR) with Routers & Switches or Equivalent	
33	Should automatically discover remote peers, reducing configuration steps.	
34	Should support configuration backup and restore in event of hardware failure by using central management device	
35	Should support environments with redundant WAN links, redundant routers, and asymmetric routing to improve high availability and optimization efficiency	
36	Should be completely transparent to different type of routing including Static routing, Dynamic routing, optimized routing etc	
37	Should integrate with existing IPSec VPN framework architecture .As on date the IPSEC/3DES is enabled between Bank's branches and Data Centers.	
38	Branch Wan Optimizer: Branch solution should have WAN optimization functionality from day one through external appliance for supporting minimum of 150 Concurrent TCP Connections for each of 4 No of International Branches with concurrent users minimum 30 per branch.	

	WAN Optimization solution should have the capability to seamlessly integrate & optimize IPsec VPN interested traffic along with application acceleration supporting applications i.e. Finacle, ATM, Mail Messaging (Exchange 2010), WEB Portal, etc. originating from Branch/office locations. The WAN Optimization solution is being procured for 4 international Branches.	
39	Attach solution document containing detailed bill of material (make, model, OS details: version, date of release, date of release of next version, end of sale & support date, product development path, etc.)	
40	Solution should integrate seamlessly with Bank's existing network Infrastructure.	

Required Minimum Technical Features of Leased Line Modem Table I

Sl. No.	Required Featured by the Bank	Yes/No
1	The modems should be TEC/DOT Type approved. Bidder has to submit the documentary evidence to support his claims.	
2	Standalone or Rack Mountable Modems, with suitable cabling are required for the bank locations for installation at bank locations and service provider end.	
3	The modems at the bank locations and service provider end should support the : V.35 Modem at CPE (Consumer Premise End) Modem should support x.21, V.35 DCE/DTE interface or E1 Interface, G.703 Modem at Service Provider End	
4	Should Operates in Full Duplex mode over 2- wire/4 wire Lines, enabling service over any copper infrastructure	
5	Operates at multiple data rates between 64 Kbps and 2MBPS	
6	Modular plug and play DTE interfaces for maximum flexibility and efficient stock management.	
7	Various DTE interfaces Like: X.21, V.35, RS-530, and G.703/G.704 E1/T1.	
8	Management via: V.24/RS-232 terminal port/ 10/100BaseT out of Band Management, Dial In, Dial Out	
9	Provides extensive diagnostics, including loop backs, SHDSL and E1 performance monitoring. Should Support SNMP agent, Should support telnet and Web Browser.	
10	Loopbacks: Local analog loopback in compliance with ITU V.54. b) Remote digital loopback in compliance with ITU V.54	
11	LEDs for power, line & loopback	
12	Attach solution document containing detailed bill of material (make, model, OS details: version, date of release, date of release of next version, end of sale & support date, product development path, etc.)	
13	Solution should integrate seamlessly with Bank's existing network Infrastructure.	

Required Minimum Technical Features of Internet Proxy Solution Table J

Sl. No.	Required Featured by the Bank	Yes/No
1	The proxy solution must Appliance based and support minimum of 2000 concurrent users from the day one and scalable up to 4000 concurrent. Centralized proxy solution should be installed at Kolkata DC. Initial Bank will procure 500 concurrent licenses for proxy server. In future bank will procure additional license in 500 blocks.	
2	The solution should be a on premise Secure Web Gateway solution having Proxy, user based URL filter, user based Application filtering on mobile devices like blocking of WhatsApp, Caching, SSL Inspection, Anti-Virus, Antimalware, spyware blocking, blocking of Peer-Peer applications like Kazaa, Gnutella, Bit Torrent, IRC (over HTTP) , including blocking of video, audio and real-time protection against zero day threats all in one solution (Appliance or software installed in Server).	
3	The solution should have the feature of Anti-Phishing, Real-time Security Scanning, URL Database Filtering, and Malicious Browser Codes, Application, Protocol Control and Classification, Scanning and filtering of Real-Time Social Networking and Web 2.0 Security like Facebook, LinkedIn, and other Web 2.0 destinations.	
4	The solution will be deployed on physical servers (not Virtual systems) / appliance and should be manageable through single unified management console. Solution should support Real-Time Security Scanning and near real time session tracking should be available in logs.	
5	The solution should monitor all HTTP and HTTPS traffic. Should detect & block spyware access to the Internet	
6	The solution should be capable to enforce safe-search restrictions for major image search engines, independent of cookies or other settings on the client machines	
7	The solution should have forward and reverse proxy and caching facility including but not limited to	

	<ul style="list-style-type: none"> • HTTP • Native FTP • FTP Over HTTP 	
8	The solution should be able to support split DNS to utilize internal and external DNS	
9	The solution should support protocol tunneling	
10	The solution should block binary executable, script based exploits, key loggers etc. that are directed towards the bank's network	
11	The solution allows override entries to be specified with wildcards within the URL. At a minimum, wildcards should be allowed at the beginning of the URL – e.g., *.xyz.com.	
12	The solution should allow override entries to be added by administrators without requiring restart of the system.	
13	The solution should be possible to optimized bandwidth usage for specific categories, applications, protocols and user.	
14	The solution should support different deployment modes.	
15	The supplied solution should support HIGH AVAILABILITY mode.	
16	The solution must identify and block webpages with: <ul style="list-style-type: none"> a. Malicious JavaScript / VB Script b. Malicious (or unauthorized) ActiveX applications c. Block Potentially Unwanted Programs (PUPs) d. Malicious Windows executable 	
17	The solution should be able to block proxy avoiding applications/software/websites such as TOR, Ultrasurf, GhostSurf, JAP, RealTunnel etc	
18	The solution should provide proxy, caching, on box malware inspection, content filtering, SSL inspection, protocol filtering on the same device/server.	
19	The solution should have IP spoofing to provide accurate representation of the IP addresses as it exits the proxy	
20	The solution should support all network communication/application protocols & ports like http, https, ftp, sftp. Bank email service should be run through proxy using gateway.	
21	The solution must identify and block configurable search strings like: porn, adult, hacking, download, shareware, etc.	
22	The solution must have in built segment wise URL database like Govt., Technical, financial, Shopping, social media etc., for blacklists like Phishing, Malicious, etc. on URL categories. Solution must have real time update.	
23	The solution should have gateway level Antivirus and malware protection	
24	The solution must have flexibility to protect from objectionable, offensive content such as (not limited to) - Religious bias sites - Gambling sites - Hacking sites etc.	
25	The solution must provide file filtering for upload/download.	
26	The solution must support different types of compression algorithms and scan nested compressed files.	
27	The solution must have flexibility to monitor and block instant messaging (IM) based file transfer and other granular controls in applications	
28	The solution must provide Web reputation as well as content based blocking/filtering	
29	The solution must be updated automatically with the new signatures from the web at customized user defined interval. <ul style="list-style-type: none"> A) Virus, B) White list/Blacklist URLs database C) System patches must be made available as and when new stable release is available D) Botnets E) Rootkits F) Malware G)Torr IP Address 	
30	The solution must have stringent security to safeguard itself against any attacks from Internet or Intranet.(like Multiple TCP Connections etc.)	
31	The solution must immediately block and alert the user if the content being downloaded/uploaded/accessed is found to contain virus/other malware.	
32	The solution must support, control and recognize al Web application traffic and protect against Web based attacks over HTTP and HTTPS.	
33	The solution should allow access based on usage time limit. Configurable for each user/group.	
34	The appliance/Software solution should send an alert message to the user, if he/she is trying to access a blocked website or a monitored website. The Message should be configurable by administrator.	
35	The solution must be capable of dynamically blocking a legitimate website which has become infected and unblock the site when the threat has been removed.	
36	The solution should perform dynamic content inspection of web-based content being accessed	

	from otherwise unblocked websites.	
37	The solution should detect and blocks outbound Botnet and Trojan malware communications. It should log and provide detailed information on the originating system sufficient to enable identification of infected units for mitigation	
38	The solution should provide real-time classification of uncategorized websites	
39	The Solution should have authentication system (User ID & Password) for accessing website based on IP address of clients.	
40	The solution should have real-time content scanning ability to understand malicious content besides on-box AV and anti-malware	
41	The solution should have ability to detect and block proxy anonymizer services.	
42	The solution should allow for delegable system administration (such as allowing for a user to configure filtering and logging for only their Active Directory or customized group without affecting the remainder of the users).	
43	The solution should provide creation of custom policies to be applied for specific user/s, IP's and group/s.	
44	The solution should provide functionality to schedule access to URL categories for specific user / users / group/groups/client /clients to access internet on specific Time/Day / Date / Weekly /Monthly etc.	
45	The solution should control incident access based on role and policy violated. The system should also allow a role creation for not having rights to view the identity of the user and the forensics of the incident	
46	The solution should create separate roles for technical administration of servers, user administration, policy creation and editing	
47	The solution should have options to create a role to see summary reports, trend reports and high-level metrics without the ability to see individual incidents	
48	The solution should allow incident managers and administrators to use their Active directory credentials to login into the console	
49	The solution should provide multiple administrator roles for configurable administrative functions	
50	The solution should provide Command-Line access for administrative purposes.	
51	The solution must have basic system health alerts to ensure availability and the capability for advanced policy alerts to enable real-time management.	
52	The solution should have Multi-Domain authentication to allow the admin to create rules that authenticate against multiple domain controllers in a sequence	
53	The Solution should be able to poll the Domain controllers to identify users logon information to transparently identify users.	
54	The solution should provide visibility into web activities as they happen, enabling proactive security. It should have capabilities to detect malware, spyware, BOT's, malicious codes real time and all inspection and scanning .	
55	The solution should support real time graphical and chart based dashboard for the summary of activities over Web	
56	The solution must provide report of the following items : IP address of client workstation, site denied access, reason of denial, time and date of denial.	
57	The Solution should have capability to provide detailed investigation reports like Risk classes - Security risk, Legal Liability risk, Bandwidth loss, productivity loss & business loss.	
58	The solution should create custom reports on a granular and/or enterprise level such as (but not limited to): <ul style="list-style-type: none"> · Usage Report of Specific User/IP/Group based on Time/Date · Report for all users who have been accessed the specific URL · Usages report based on Time & Date · Top service user · Most requested service 	
59	The solution must provide a clear and detailed reporting mechanism that users can leverage for investigations and usage reports. The reports templates should be customizable and must be flexible in filtering by various data types (IP range, subnet, users).	
60	The solution should be able to generate & export or email reports automatically to assigned users in various formats: - PDF, - HTML - Excel/CSV	
61	The solution must support granular access control and authorization to facilitate gathering log information of users.	
62	All usage reports must be able to be run daily, weekly, monthly, quarterly, semi-annually, and annually, or a configurable time span.	
63	All usage reports must be capable of running automatically and delivered to designated personnel via electronic means	

64	The solution should provide read only accounts to view logs and reports.	
65	The solution must provide reports to track the performance of this system including an event log showing any system down time or system exceptions or other problems.	
66	The system should allow reports to be mailed directly from the UI and should allow automatic schedule of reports to identified recipients	
67	The reports should be exported to at least CSV, PDF, HTML formats	
68	The system should provide options to save specific reports as favorites for reuse.	
69	The system should have lots of pre-defined reports which administrators can leverage	
70	The solution should have capabilities to detect custom encrypted payloads, password files and other identified sensitive information getting stolen through modern malware.	
71	The solution should be able to detect encrypted and password protected files in any known/unknown encrypted format	
72	The solution should have anti-malware engines(Signature and Heuristics based) and should also have capabilities to inspect malware embedded in PDF files	
73	The solution should support future addition of Malware Sandbox functionality to evaluate the malicious code and provide detailed report on analysis.	
74	The solution should be able to detect data theft even if the malware sends the data through image files.	
75	The solution should provide geo destination awareness so the location where the malware is trying to establish connection can be tracked.	
76	The solution should have the ability to detect sensitive content embedded in image files over Web channel	
77	The solution should be able to detect encrypted and password protected files.	
78	The solution should be able to recursively inspect the content of compressed archives	
79	The solution should be able to identify malicious traffic pattern generated by Malware infected PC in order to prevent future data leakage by the malware	
80	The solution should be capable of detecting data-thefts by any malicious activity in the network by a malware or other security threat.	
81	The solution should be able to enforce policies by URL's, domains or URL categories natively – For example only HR is allowed to post Resume to Job Search sites. No sensitive content can go to malicious websites, social networking sites etc.	
82	The solution should report incident with URL category information along with user. Content violating the policy etc. to be displayed in the incident, for instance which URL category did the information should appear in the incident.	
83	The solution should have web filtering activities with geo-location information	
84	System should provide information to Administrator on infected machines and infection type	
85	System should provide Email/Text Alerts Based on Threshold Violations	
86	System should generate Reports Identifying Users by AD Name, IP.	
87	Proposed system should have at least 3 no. of 100/1000 interfaces Ethernet Interface RJ45 and solution should have WAN load balancing facility between two no. of internet connection.	
88	The OEM should provide 24x7 technical support through phone and Web, Product Upgrades, Updates, Patches and access to Technical Library and Product Documentation.	
89	The OEM should have its technical support center in India.	
90	The Solution should appliance based. In case any software and server required to comply all points , bidder should supply server and OS licenses with Proxy solution.	
91	The Solution should support IPv4 and IPv6 both.	
92		

Required Minimum Technical Features of AAA Solution

Table K

Sr.No.	Required Featured by the Bank	Yes/No
1	The AAA solution should be software based and should install on a standard server or AAA solution should be appliance base.	
2	This proposed solution should be able to enhance the security and manageability using centralize user authentication, configuring the appropriate access level, and ensuring compliance with enterprise security policies.	
3	It should support Authentication by validating any user's login credentials against a central security database to ensure that only individuals with valid credentials will be granted network access	
4	The proposed solution should be able to integrate with industry leading Directory server like but not limited to LDAP server, Microsoft Active Directory, RSA SecurID server, or TACACS+ server etc.	

5	It should support Authorization by Providing information to the network access device for each new connection (e.g., what IP address to use, session time-limit information, or which type of tunnel to set up)	
6	It should support Accounting and should Log all connections, including user names and connection duration, for tracking and billing	
7	The proposed solution should: Centrally enforce network access and security policies. Control who is authorized to access the network. Configure restrictions or special characteristics of user access, such as connection time limits or a requirement to meet a certain wireless security level.	
8	The proposed solution should provide reporting and statistics on network activity, for readily available diagnostics.	
9	The proposed solution should be compatible with SNMP-based management systems.	
10	The proposed solution should support features such as GUI and replication to DR Site for simple configuration and maintenance.	
11	Enable configuration either programmatically or at the command line prompt.	
12	It should support the replication of AAA configuration data from a primary server to multiple replica servers within a replication realm.	

All above devices must be IPV6 compliant from day 1 and should support the all IPV6 functionality.

Annexure -J**Technical Template**

New Network Equipment with 3 years Warranty & support			Table A
Sl No.	Description	Qty.	
1	Router Type A	300	
2	24 Port Switch Type B	300	
3	64Kbps/128Kbps/256 Kbps/ 512Kbps/2Mbps Modem	300	

Link implementation for 3 Years			Table B
Sl No.	Description	Qty.	
1	New link (MPLS/P2P) implementation including backup link	300	

Link upgradation and shifting for 3 years			Table C
Sl No.	Description	Qty.	
1	Link shifting	300	
2	Link upgradation	1000	
3	128Kbps/256 Kbps/ 512Kbps/2Mbps Modem	1000	

##Network Link Management Service				Table D
Sl. No.	Network Area	Link Type	Qty.	
1	Branch Network	MPLS Link	2662	
2		ISDN BRI	1125	
3		ISDN PRI	15	
4		CDMA	487	
6	Core Network	MPLS Link	6	
7		P2P link	8	

Present nos. of links in each type is mentioned above. However the nos. of links may vary (increase or decrease) in future. Bank will pay cost of link management service based on the link type available /managed by the bidder at that time.

**Comprehensive AMC for 3 years			Table E		
Make	Model	Qty.	1st Year	2nd Year	3rd Year
HP	HP 6608	4	Yes	Yes	Yes
HP	MSR 30-20 JF284A	4	Yes	Yes	Yes
HP	MSR 30-40 JF229A	2	Yes	Yes	Yes
HP	HP A5120-48G EI	13	Yes	Yes	Yes
HP	HP 7500 Advanced VPN Firewall Module JD249A	8	Yes	Yes	Yes
HP	HP A7503-S-6626	4	Yes	Yes	Yes
HP	HP A5500-24G EI	4	Yes	Yes	Yes
CISCO	Cisco 3845/Cisco2921	11	Yes	Yes	Yes
CISCO	CISCO-WS-C6509-E	4	Yes	Yes	Yes
HP	H3C MSR 930	1	Yes	Yes	Yes
HP	H3C MSR 931	1	Yes	Yes	Yes
HP	HP MSR20-11	1678	Yes	Yes	Yes
HP	HP 2510B-24	1608	Yes	Yes	Yes
HP	HP 2510B-48	43	Yes	Yes	Yes
HP	HP 2530-24	207	Yes	Yes	Yes
HP	HP A3100-8	859	Yes	Yes	Yes
F5	F5-BIG-LC-1600-4G-R	1	Yes	Yes	Yes

Check Point with IPS (HA)	Power-1 5077 with IPS (HA)	4(HA)	Yes	Yes	NA
Check Point (HA)	UTM-1 574 (HA)	4 (HA)	Yes	Yes	NA
Check Point	Check Point Management software R77.30	2	Yes	Yes	NA
CISCO	ACS 1121	2	Yes	Yes	NA
Riverbed	Sheelhead SHA 1050	8	Yes	Yes	NA
Remote VPN license for Check Point Power 5077	Remote VPN license for Check Point Power 5077	200	Yes	Yes	NA

** Replacement of Old product					Table F		
Sl. No.	Old Make/Model	Qty.	New Replacement device Make/Model	Qty.	Replacement Year		
					1 st Year	2 nd Year	3 rd Year
1	Cisco 1760	152	Specification as per Type A Router in Annexure G	152	Yes	NA	NA
2	Cisco 1841	825	Specification as per Type A Router in Annexure G	825	Yes	NA	NA
3	Cisco 871	300	Specification as per Type A Router in Annexure G	300	Yes	NA	NA
4	HP Procurve 7102 DL	189	Specification as per Type A Router in Annexure G	189	Yes	NA	NA
5	Cisco2821/2851	17	Specification as per Type B Router in Annexure G	17	Yes	NA	NA
6	Cisco 7204VXR/ 7206VXR	3	Specification as per Type C Router in Annexure G	3	Yes	NA	NA
7	FWSM(WS-SVC-FWM-1-K9)	4	ASA Services Module for Catalyst 6500-E, 3DES/AES	4	Yes	NA	NA
8	Cisco ASA 5550 (HA)	2(HA)	Specification as per Firewall in Annexure G	2 (HA)*	Yes	NA	NA
			Specification as per IPS in Annexure G	2 (HA)*	Yes	NA	NA
9	CISCO-WS-C3550-24-SMI/ WS-C3560G-24TS/ WS-C3750G-24T/ WS-C3750G-48TS	19	Specification as per Switch Type A in Annexure G	19	NA	Yes	NA
10	Check Point UTM-1 574 (HA)	4 (HA)	Specification as per Firewall in Annexure G	4 (HA)*	NA	NA	Yes
			Specification as per IPS in Annexure G	4 (HA)*	NA	NA	Yes
11	Check Point Power 5077 with IPS (HA)	4 (HA)	Specification as per Firewall in Annexure G	4 (HA)*	NA	NA	Yes
			Specification as per IPS in Annexure G	4 (HA)*	NA	NA	Yes
12	Check Point Management software R77.30	2	Specification as per Firewall in Annexure G	2	NA	NA	Yes
13	Cisco ACS 1121	2	Specification as per AAA solution in Annexure G	2	NA	NA	Yes
14	Sheelhead SHA 1050	8	Specification as per WAN optimizer in Annexure G	8	NA	NA	Yes
15	Remote VPN license for Check Point Power 5077	200	Specification as per Firewall in Annexure G	200	NA	NA	Yes

* Bidder may supply & installed IPS inbuilt with Firewall in same appliance without any Performance issue and should comply all technical requirement of Firewall & IPS as per Annexure G.

Bidder must have back to back support relation with the OEM's whose products are followed by the bidder to the Bank, in case the bidder is not Original Equipment Manufacturer(OEM). **A commitment letter from the OEM(s) as per Annexure-C has to be submitted along with the Technical bid in this regard at least for a period of 5 years for all new & AMC related network equipment as per Annexure J

***Warranty period for 1st year Replacement product – 3 Years
 2nd year Replacement product – 2 Years
 3rd year Replacement product – 1 Years

**Centralized Proxy Solution with 3 years Warranty & support			Table G
Sl. No.	Product details	Qty.	New Replacement device Make/Model
1	Proxy solution with Hardware of 2000 concurrent user support with 500 user licenses	1	
2	Upgradation hardware for additional 2000 concurrent user	1	
3	License for 500 user licenses block	7	

Bidder must have back to back support relation with the OEM's whose products are followed by the bidder to the Bank, in case the bidder is not Original Equipment Manufacturer(OEM). **A commitment letter from the OEM(s) as per Annexure-C has to be submitted along

Commercial Template

New Network Equipment with 3 years Warranty & support															Table A
SI No.	Description	Make/M odel /Part No.	1 st Year with 3 years warranty				2 st Year with 2 years warranty				3 rd Year with 1 years warranty				Total D4=D1+D2+ D3+D4
			Qty. (a1)	Unit Price (b1)	%Tax es (c1)	Total Price including taxes D1 = a1 X (b1 + b1 X c1)	Qty. (a2)	Unit Price (b2)	%Tax es (c2)	Total Price including taxes D2 = a2 X (b2 + b2 X c2)	Qty. (a3)	Unit Price (b3)	%Taxe s (c3)	Total Price including taxes D3 = a3 X (b3 + b3 X c3)	
1	Router Type A		100				100				100				
2	24 Port Switch Type B		100				100				100				
3	64Kbps/128Kbps/256 Kbps/ 512Kbps/2 Mbps Modem		100				100				100				
Sub Total (A)															

Link implementation for 3 Years					Table B
SI No.	Description	Qty. (a)	Unit Price (b)	%Taxes (c)	Total Price including taxes d = a X (b + b X c)
1	New link implementation including backup link	300			
Sub Total (B)					

Link upgradation and shifting for 3 years					Table C
SI No.	Description	Qty. (a)	Unit Price (b)	%Taxes (c)	Total Price including taxes d = a X (b + b X c)
1	Link shifting	300			
2	Link upgradation	1000			
3	128Kbps/256 Kbps/ 512Kbps/2Mbps Modem	1000			
Sub Total (C)					

Network Link Management Service*													Table D
Sl. No.	Network Area	Link Type	Qty. (a)	1 st Year			2 nd Year			3 rd Year			Total in 3 Years including taxes D4=D1+D2+D3
				Unit Price (b1)	%Taxes (c1)	Total Price including taxes D1 = a X (b1 + b1 X c1)	Unit Price (b2)	%Taxes (c2)	Total Price including taxes D2 = a X (b2 + b2 X c2)	Unit Price (b3)	%Taxes (c3)	Total Price including taxes D3 = a X (b3 + b3 X c3)	
1	Branch Network	MPLS Link	2662										
2		ISDN BRI	1125										
3		ISDN PRI	15										
4		CDMA	487										
6	Core Network	MPLS Link	6										
7		P2P link	8										
Sub Total (D)													

*Present nos. of links in each type is mentioned above. However the nos. of links type may vary (increase or decrease) in future. Bank will pay cost of link management service based on the link type available /managed by the bidder at that time.

Comprehensive AMC for 3 years													Table E
Sl. No.	Make	Model	Qty.	1 st Year			2 nd Year			3 rd Year			Total in 3 Years including taxes D4=D1+D2+D3
				Unit Price (b1)	%Taxes (c1)	Total Price including taxes D1 = a X (b1 + b1 X c1)	Unit Price (b2)	%Taxes (c2)	Total Price including taxes D2 = a X (b2 + b2 X c2)	Unit Price (b3)	%Taxes (c3)	Total Price including taxes D3 = a X (b3 + b3 X c3)	
1	HP	HP 6608	4										
2	HP	MSR 30-20 JF284A	4										
3	HP	MSR 30-40 JF229A	2										
4	HP	HP A5120-48G EI	13										
5	HP	HP 7500 Advanced VPN Firewall Module JD249A	8										
6	HP	HP A7503-S-6626	4										

7	HP	HP A5500-24G EI	4										
8	CISCO	Cisco 3845/Cisco2921	11										
9	CISCO	CISCO-WS-C6509-E	4										
10	HP	H3C MSR 930	1										
11	HP	H3C MSR 931	1										
12	HP	HP MSR20-11	1678										
13	HP	HP 2510B-24	1608										
14	HP	HP 2510B-48	43										
15	HP	HP 2530-24	207										
16	HP	HP A3100-8	859										
17	F5	F5-BIG-LC-1600-4G-R	1										
18	Check Point	Power-1 5077 with IPS	4 (HA)							NA	NA	NA	
19	Check Point	UTM-1 574	4(HA)							NA	NA	NA	
20	Check Point	Check Point Management software R77.30	2							NA	NA	NA	
21	CISCO	ACS 1121	2							NA	NA	NA	
22	Riverbed	Sheelhead SHA 1050	8							NA	NA	NA	
23	Remote VPN license	Check Point Power 5077	200							NA	NA	NA	
Sub Total (E)													

Replacement of Old product**					Table F					
Sl. No.	Old Make/Model	Qty.	New Replacement device Make/Model	Qty. (a)	Unit Price of device (b)	%Taxes (c)	Unit price installation per device (d)	%Taxes (e)	Total Price including taxes d = a X [(b + b X c) +(d+ d x e)]	
1	Cisco 1760	152	Specification as per Type A Router	152						

			in Annexure G						
2	Cisco 1841	825	Specification as per Type A Router in Annexure G	825					
3	Cisco 871	300	Specification as per Type A Router in Annexure G	300					
4	HP Procurve 7102 DL	189	Specification as per Type A Router in Annexure G	189					
5	Cisco2821/2851	17	Specification as per Type B Router in Annexure G	17					
6	Cisco 7204VXR/ 7206VXR	3	Specification as per Type C Router in Annexure G	3					
7	FWSM(WS-SVC-FWM-1-K9)	4	ASA Services Module for Catalyst 6500-E, 3DES/AES	4					
8	Cisco ASA5550 (HA)	2 (HA)	Specification as per Firewall in Annexure G	2 (HA)					
			Specification as per IPS in Annexure G	2 (HA)					
9	CISCO-WS-C3550-24-SMI/ WS-C3560G-24TS/ WS-C3750G-24T/ WS-C3750G-48TS	19	Specification as per Switch Type A in Annexure G	19					
10	Check Point UTM-1 574 (HA)	4(HA)	Specification as per Firewall in Annexure G	4(HA)					
			Specification as per IPS in Annexure G						
11	Check Point Power 5077 with IPS (HA)	4(HA)	Specification as per Firewall in Annexure G	4 (HA)					
			Specification as per IPS in Annexure G						
12	Check Point Management software R77.30	2	Specification as per Firewall in Annexure G	2					
13	Cisco ACS 1121	2	Specification as per AAA solution in Annexure G	2					
14	Sheelhead SHA 1050	8	Specification as per WAN optimizer in Annexure G	8					
15	Remote VPN license	Check Point Power 5077	Specification as per Firewall in Annexure G	200					

Sub Total (F)

- **
- SI No 1 to 8 unit price with 3 years warranty.
 - SI No. 9 unit price with 2 years warranty.
 - SI No. 10 to 14 unit price with 1 year warranty.

Centralized Proxy Solution with 3 years Warranty & support					Table G
Sl. No.	New Replacement device Make/Model	Qty. (a)	Unit Price (b)	%Taxes (c)	Total Price including taxes $d = a \times (b + b \times c)$
1	Proxy solution with Hardware of 2000 concurrent user support with 500 user licenses#	1			
2	Upgradation of Hardware additional 2000 concurrent user	1			
3	License Cost for 500 user licenses block#	7			
3	Implementation cost	1			
Sub Total (G)					

Bidder should quote license cost for 3 years, but bank will pay on pro-data basic.

Grand Total		Table H
Sl.No.	Description	Total
1	New Network equipment with 3 Years Warranty (A)	
2	New Link implementation (B)	
3	Link upgradation and shifting in 3 years (C)	
4	Network Management Service (D)	
5	Comprehensive AMC for 3 years (E)	
6	Replacement of old network device (F)	
7	Centralized Proxy Solution (G)	
Grand Total H=A+B+C+D+E+F+G		

Note:

1. In case of discrepancy between figures and words, the amount in words shall prevail.
2. Bidders should strictly quote in the format and for periods as mentioned above. No counter condition/assumption in response to commercial bid will be accepted. Bank has a right to reject such bid.
3. **The bidder with lowest commercial cost in Table H (Grand Total H) above will be selected as L1 bidder.**
4. In the event the vendor has not quoted or mentioned any component or services required, for evaluation purposes the highest value in the submitted bids for that particular link type would be used to calculate the TCO. For the purposes of payment and finalization