Sl. No.	Category	Section	RFP Clause	Page No.	Clause/Technical Specification	Bidder's Query	Response to Query
1	Generic	Bidder's responsibility	5.3	8	The bidder/OEM must analyse the existing production system and gather performance metrics. The bidder/ OEM should recommended changes as per best practices wherever applicable	Does bank has any ready performance metrics like , No. of connections per day, User counts per day, Data recevied and sent, Cache reports,Number of HTTP/S requests received? Please share	Bidder to comply with RFP terms
2	Generic	Additional Points	Additional Query	N/A	N/A	The Web Security/DLP will be highly vulnerables if text on Image Files (Screenshots/Scanned Files) can not be analyzed. This feature is critical specifically for Banking and is part of most of the Bank RFPs including Canara Bank Web Security (SWG) RFP: The solution should have the ability to detect sensitive content embedded in image files over Web channel	Not required
3	Generic	Additional Points	Additional Query	N/A	N/A	Solution should support off the network roaming users (Remote Filtering) and On-the-network (corporate) users. For roaming users connecting to Internet via Data card, WIFI, the corporate proxy policies should be enforced on them. Remote Filtering option has to be made with on premise solution only.	Not required
4	Generic	Additional Points	Additional Query	N/A	N/A	To decrypt the SSL traffic, proxy certificate need to be present on the end user browser, will bank will provide & use the Trutsted CA certifiate present on the system or use the proxy self signed certificate. In case using self sign certificate Bank need to ensure it present on the end user's browsers	Bank will use self signed certificate, bidder shall be required to size, supply, implement, maintain and manage in accordance.
5	Generic	Additional Points	Additional Query	N/A	N/A	how currently client browser sending web request to proxy, eg, using pac file, proxy ip and port configured on the individual browser, traffic routed from network device.	Using IP address and Port of Proxy service
6	Generic	Additional Points	Additional Query	N/A	N/A	Curretnly internet polices are maintained offline in spreesheet, word file? Is it possiable to export the polices from exisitng proxy solution in the format of Source, Destination, Action	Would be shared with the successful bidder
7	Generic	Additional Points	Additional Query	N/A	N/A	Bank will be using this solution in Forward proxy mode or reverse proxy mode?	Forward proxy for internet browsing.
8	Generic	Additional Points	Additional Query	N/A	N/A	The Web Security/DLP will be highly vulnerables if text on Image Files (Screenshots/Scanned Files) can not be analyzed. This feature is critical specifically for Banking and is part of most of the Bank RFPs including Canara Bank Web Security (SWG) RFP: The solution should have the ability to detect sensitive content embedded in image files over Web channel	Bidder to comply with RFP terms
9	Generic	Bidder's responsibility	5.13	8	Solution should have capability to integrate with other security solutions, as and when implemented by Bank such as SIEM, etc	What is current SIEM Solution implemented at Bank ?	Bidder to comply with RFP terms
10	Generic	Bidder's responsibility	5.5	8	Configuration of the security polices within the Secure Web Gateway solution as per the Banks requirement and Solution should support policies as per user names, groups, IP or IP ranges and time bound	What is the source of users information? Does envrionment has Microsoft Active Directory or other directory service	Bank has Microsoft Active Directory service.
11	Generic	Detailed Scope of Work for the Bidder	5	8	The bidder/OEM must analyse the existing production system and gather performance metrics. The bidder /OEM should recommended changes as per best practices wherever applicable.	As per Bidders understanding the scope is limited to Secure Web Gateway recommendations only. Please clerify.	Bidder is required to size, supply, implement, integrate, maintain and manage the solution.

12	**Generic**	**Detailed Scope of Work for the Bidder**	**5**	8	Configuration of the security polices within the Secure Web Gateway solution as per the Banks requirement and Solution should support policies as per user names, groups, IP or IP ranges and time bound	Does Bank has documented the Business Functional & Non-functional Business Requirements pertaining to Security Policies. If yes; please share the same for feasibility and adoption requirement purposes.	Would be shared with the successful bidder
13	**Generic**	**Eligibility Criteria**	**Bidder 8**	49	The bidder should have successfully implemented the proposed / similar class of Secure Web Gateway solution of the same OEM in atleast 1 Government Department/PSU/ Public Sector Bank environment with minimum 100 branches/ offices in India during last three financial years:- - 2016 to 2017 - 2017 to 2018 - 2018 to 2019 Proof of Concept (POC) done will not be treated as experience of the bidder	Requesting to change to "The bidder should have successfully implemented the proposed / similar class of Secure Web Gateway solution atleast 1 Government Department/PSU/ Public Sector Bank/Private Sector Bank environment with minimum 100 branches/ offices in India during last three financial years:- - 2016 to 2017 - 2017 to 2018 - 2018 to 2019 Proof of Concept (POC) done will not be treated as experience of the bidder	Refer to RFP-Addendum Item 1
14	**Generic**	**Eligibility Criteria**	**OEM 1**		The proposed solution should be currently live in a Bank in India - Supporting Documents Relevant Credential letters OR Purchase Order along with Self Declaration certifying to that effect, signed by CFO / Person Authorized by CFO, along with the seal of the Bidder's company / firm.	The proposed solution should be currently live in any BFSI customer	Bidder to comply with RFP terms
15	**Generic**	**Eligibility Criteria**	**OEM 2**		The proposed secured web gateway appliance should not have been declared end of sale as on last date of bid submission and must be under OEM support for the contract period Self- Declaration on OEM's letter head		No Query
16	**Generic**	**Eligibility Criteria**	**OEM 3**		Web security solution OEM must be listed in the "Leaders" or "Challengers" Quadrant of the latest available Gartner Magic Quadrant for Secure Web Gateways solution. Latest Gartner Magic Quadrant report for Secure Web Gateway		No Query
17	**Generic**	**Eligibility Criteria**	**Bidder 8**	50	Government Department/PSU/ Public Sector Bank environment with minimum 100 branches/ offices in India	We request that the minimum branches / offices should be made to 500+ considering the size of your Bank.	Bidder to comply with RFP terms
18	**Generic**	**Eligibility Criteria**	**Bidder 2**	**49**	The Bidder should have a minimum turnover of Rs. 100 (One Hundred) Crores per annum from IT sales in each of the last three financial years In India. Ie 2016-17 2017-18 2018-19	Request Bank to amend this **Rs.50 (Fifty) Crores** per Annum from IT Sales in each of the Last 3 years in India.	Refer to RFP-Addendum Item 2

19	**Generic**	**Eligibility Criteria**	**Bidder 8**	**50**	The bidder should have successfully implemented the proposed / similar class of Secure Web Gateway solution of the same OEM in atleast 1 Government Department/PSU/ Public Sector Bank environment with minimum 100 branches/ offices in India during last three financial years:- - 2016 to 2017 - 2017 to 2018 - 2018 to 2019	Request Bank to Amend this as "The bidder should have successfully implemented the **proposed / similar class of Secure Web Gateway solution in atleast 1** Government Department/PSU/ Public Sector Bank environment/**BFSI/Public Listed Company** in India during last three financial years:- - 2016 to 2017 - 2017 to 2018 - 2018 to 2019"	Refer to RFP-Addendum Item 1
20	**Generic**	**Eligibility Criteria**	**Bidder 8**	50	The bidder should have successfully implemented the proposed / similar class of Secure Web Gateway solution of the same OEM in atleast 1 Government Department/PSU/ Public Sector Bank environment with minimum 100 branches/ offices in India during last three financial years:- - 2016 to 2017 - 2017 to 2018 - 2018 to 2019 Proof of Concept (POC) done will not be treated as experience of the bidder	Softcell Technologies has Successfully implemented the proposed / similar class of Secure Web Gateway solution of other OEMs' who are Leaders in Gartner Quadrant (this can be substantiated by providing relevant PO copies and implementation). In this case we would like to align with a different OEM of the same solution. Hence we request Bank to amend this Clause by Removing SAME OEM in atleast 1Government Department /PSU / PublicSector Bank environment withminimum 100 branches / offices / Corporates / Private Enterprise inIndia during last FOUR financialyears:- - 2015 to 2016 - 2016 to 2017 - 2017 to 2018 - 2018 to 2019	Refer to RFP-Addendum Item 1
21	**Generic**	**Eligibility Criteria**	**Bidder 2**	49	The Bidder should have a minimum turnover of Rs. 100 (One Hundred) Crores per annum from IT sales in each of the last three financial years In India. Ie 2016-17 2017-18 2018-19 **Supporting documents** Audited Financial statements for the financial years in concern AND CA Certificate indicating the IT sales Turnover for the previous financial years mentioned above.	For the Financial Year 2018-19 Audit is in progress, Requested to accept Un-Audited CA certificate.	Refer to RFP-Addendum Item 3
22	**Generic**	**Installation and configuration**	**7.2**	12	All the installation and configuration shall be under the direction and guidance of the OEM.	Does this means that I&C shall be vetted by OEM	Bidder to comply with RFP terms
23	**Generic**	**Installation and configuration**	**7.2.7**	**13**	The implementation will be deemed complete when all the supplied devices including hardware, operating systems, licenses, database, supporting software, drivers, etc are installed and accepted by the Bank. The new Secure Web Gateway should be configured with all the policies and moved to the production environment	How many Polices to be configure before moving to production environment? Request bank to provide the total number of polices	Bidder to comply with RFP terms
24	**Generic**	**Monitoring and Management**	**6.6**	10	The proposed solution should be managed centrally through a single Management Console.	Bidder recommends to use separate Management Console for DC/DR Sites. Once DC is down the Management Console Server will also be down. So, there is the necesscity to have separate Management Console Server.	Bidder to comply with RFP terms

25	**Generic**	**Monitoring and Management**	**6.6.2.2**	**10**	The management platform should be configured to proactively detect the health issues and service degradation/interruptions and should be able to create event / alerts to the relevant administrators through Email, SMS etc.	Events and alerts available through Email, Syslog. Request bank to remove SMS notification	Bidder to comply with RFP terms
26	**Generic**	**Payment Terms**	**11.4.1, 11.4.2, 11.4.3**	**37**	Delivery of Solution and on production of relevant documents:- 70% of total order value. Installation, Configuration and Commissioning :- 20% of total order value. Warranty - 10% of total order value	Request Bank to amend this as "Delivery of Solution and on production of relevant documents:- 80% of total order value. Installation, Configuration and Commissioning :- 10% of total order value. Warranty - 10% of total order value	Bidder to comply with RFP terms
27	**Generic**	**Payment terms/ Payment Milestones:**	**11, 11.4**	37	11.4.1 Delivery of Solution and on production of relevant documents:- 70% of total order value	Requested to modify the clause as "Delivery of Hardware /Software and on production of relevant documents:- 70% of total order value."	Bidder to comply with RFP terms
28	**Generic**	**Penalties for non-maintenance of uptime during the contract period**	**8.5**	14	If the Successful Bidder fails to meet the requirements under Service Level Agreement like delays/defaults/deficiency of services in delivery/ installation/replacement /repair of any or all of the Systems/equipment's /Solution mentioned in the Purchase order (PO), Bank shall, without prejudice to its other rights and remedies under and in accordance with the Contract, deduct from the Contract price, as liquidated damages, a sum equivalent to 0.5% per week or part thereof of the value of P.O. In case of undue delay beyond a period of 15 (fifteen) days unless otherwise waived by the Bank, Bank at its discretion may consider termination of the Contract. 8.5.2 Penalties for non-maintenance of uptime during the contract period 0.10% plus applicable taxes on total PO value for every hour or part thereof	There is the inconsistancy between penalty/liquidated Damage section as one states per hour & other states per week. Please clarify	Bidder to comply with RFP terms
29	**Generic**	**Penalties for non-maintenance of uptime during the contract period**	**8.5**	14	8.5.1.3 The total penalty/Liquidated damages under above clause will be restricted to a ten percent (10 %) of the total value of the contract. 8.5.2.2 The maximum penalty levied shall not be more than 25% plus applicable taxes of the AMC amount payable for one year.	There is the inconsistancy in maximum cap of penalty. As per Bidders understanding there can not be two capping under one contract. Please clarify.	Bidder to comply with RFP terms
30	**Generic**	**Penalties/ Liquidated damages**	**8.5.1.3**	14	The total penalty/Liquidated damages under above clause will be restricted to a ten percent (10 %) of the total value of the contract.	Requesting to amend the clause to "The total penalty/Liquidated damages under above clause will be restricted to a five percent (5 %) of the total value of the contract.	Bidder to comply with RFP terms
31	**Generic**	**Penalties/ Liquidated damages**	**8.5**	15	The maximum penalty levied shall not be more than 25% plus applicable taxes of the AMC amount payable for one year.	Penalty capping is very stringent. We request that the penalty should be capped to 5% Plus taxes of the AMC amount payable for one year.	Bidder to comply with RFP terms
32	**Generic**	**Support engineers**	**8.6**	15	The bidder must provide service availability of the onsite engineer at Banks' premises, specified by the Bank in the order, on all working days of both Banks.	Does onsite engineers are required at both Banks from Day1. Please clarify.	Bidder to comply with RFP terms

33	**Generic**	**Timeline**	**7.1**	12	Supply of appliance at DC and DRC of the Bank	OEM standard delivery period is 6-8 weeks from PO date. We request that delivery timelines be modified as 8 weeks from PO date.	Bidder to comply with RFP terms
34	**Generic**	**Supply of appliance at DC and DRC of the Bank**	7.1	12	Within 6 weeks from date of PO acceptance at respective locations in Bengaluru and Mumbai	request you to extend the delivery timelines to 8 weeks	Bidder to comply with RFP terms
35	**Generic**	**Appliance and related software installation, cabling**	7.1	12	Within 8 weeks from date of PO acceptance	request you to extend the delivery timelines to 12 weeks	Bidder to comply with RFP terms
36	**Generic**	**Mean Time To Restore (MTTR) for the Bidder -**	8.3	13	The bidders response time shall be less than 1 hour and the MTTR shall be less than 2 hours. Time specified above is from the time of lodging the complaint or intimation to the bidder.	request you to change the MTTR to 5 Hours since the OEM support aligned for 4 hours	Bidder to comply with RFP terms
37	**Generic**	**Penalties/ Liquidated damages**	8.5.2.2	15	The maximum penalty levied shall not be more than 25% plus applicable taxes of the AMC amount payable for one year	request to limit the maximum penalty to 10% of the AMC amount payable	Bidder to comply with RFP terms
38	**Generic**	**Payment for Support engineer**	11.5	37	Payment for Onsite support shall be released monthly in arrears, post adjusting absence, on submission of invoice and attendance certificate counter-signed by Bank official. Onsite support will commence from the date of acceptance of solution by the Bank.	request you to consider 12 days leaves for the resources in an year which has to be exempted while calculating penalty.	Bidder to comply with RFP terms
39	**Generic**	**Terms and Conditions**	12.2	38	IP Rights	Bidder can only pass on all OEM warranties in toto but not give broad warranties as stipulated. Since IP indemnity is already provided, further warranties will be onerous with risk of double dipping. Kindly acknowledge.	Bidder to comply with RFP terms
40	**Generic**	**Terms and Conditions**	12.3	38	Indemnity	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. Also please confirm that 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 carve-outs.	Bidder to comply with RFP terms
41	**Generic**	**Terms and Conditions**	NA	NA	No limitation of liability	We request Bank to cap the aggregate liability to total contract value under the applicable Purchase Order.	Bidder to comply with RFP terms
42	**Generic**	**Terms and Conditions**	12.2	44	Negligence	Kindly provide a specific timeframe (45 days) as a grace period for rectification prior to cancellation under this clause.	Bidder to comply with RFP terms
43	**Generic**	**Terms and Conditions**	12.17	43	Order Cancellation	As currently drafted the Order cancellation clause is very broad and the threshold of such cancellation is too low. Bidder requests that any cancellation of contract should be invoked only for failure to cure a material breach of contract by Bidder with 30 days written notice.	Bidder to comply with RFP terms

44	**Generic**	**Eligibility Criteria**	**Bidder 8**	50	The bidder should have successfully implemented the proposed / similar class of Secure Web Gateway solution of the same OEM in at least 1 Government Department / PSU / Public Sector Bank environment with minimum 100 branches / offices in India during last three financial years:- - 2016 to 2017 - 2017 to 2018 - 2018 to 2019 Proof of Concept (POC) done will not be treated as experience of the bidder	We request the Bank to amend the clause and accept successfully implemented similar class of solutions of Secure web gateway solution (same OEM or other) in at least 1 Government Department / PSU / Public Sector Bank environment with minimum 100 branches / offices in India during last five financial - 2014 to 2015 - 2015 to 2016 - 2016 to 2017 - 2017 to 2018 - 2018 to 2019 Proof of Concept (POC) done will not be treated as experience of the bidder	Refer to RFP-Addendum Item 1
45	**Generic**	**Eligibility Criteria**	Point 1	2	The proposed solution should be currently live in a Bank in India	Please change the specification as below: *"The proposed solution should be currently live in any BFSI customer in India"*	Bidder to comply with RFP terms
46	**Generic**	**Others**				L1 or RA bid, kinldy confirm	RA bid
47	**Generic**	**Insurance**	12.7		12.7 Insurance 12.7.1 The appliance to be supplied will be insured by the Bidder against all risks of loss or damages from the date of shipment till such time, the same is delivered, installed and accepted by Bank at site and handed over to the Bank/Office	Since Title of ownership of goods supplied under this contract will be passed on to the Bank on delivery of goods at the site, Insurance shall be till the time of delivery only.	Bidder to comply with RFP terms
48	**Generic**				Please include Deemed Acceptance clause	Products/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 bidder within 15 days from the date of installation or when Customer uses the Deliverable in its business, whichever occurs earlier. It is further clarified that any payment linked with acceptacne will be released by the Bank	Not required
49	**Generic**	**Payment Terms**	11.4		11.4 Payment Milestones: 11.4.1 Delivery of Solution and on production of relevant documents:- 70% of total order value 11.4.2 Installation, Configuration and Commissioning :- 20% of total order value Conditions:- 20% of the total cost will be released after successful implementation, integration of SWG solution supplied as per Scope of Work 11.4.3 Warranty - 10% of total order value Conditions:- 10% of the total cost shall be paid only after completion of warranty period of 3 years, or , on submission of a BG for equivalent amount by the vendor after completion of 90% payment	we request that 2nd milestone of the payment(20% of the total cost) shall be released on successful installation which is 8 weeks from the PO acceptance & 3rd milestone (last 10% of the total cost)after successful implementation which is 4 month from the acceptance of PO.	Bidder to comply with RFP terms
50	**Generic**	**Payment Terms**			11.5 Payment for Support engineer Payment for Onsite support shall be released monthly in arrears, post adjusting absence 11.3 AMC would be paid in quarterly arrears and ATS would be paid yearly in advance	We request; Payment for Onsite support shall be released monthly in advance 11.3 AMC shall also be paid in Yearly advance	Bidder to comply with RFP terms

51	**Generic**	**Payment Terms**			9.4.4 Beyond the quantities mentioned in the RFP Appendix 1 – Bill of materials, the Bank reserves the right to increase or decrease the quantum of purchase by 25%, at the same unit rates and same Terms and Conditions of this tender. All the Hardware/Software should have comprehensive onsite warranty of 3 years and AMC support of 2 years	We request to limit the increase or decrease the quantum of purchase by 10%, at the same unit rates and same Terms and Conditions if ordered within Bid validity period.	Bidder to comply with RFP terms
52	**Generic**	**Warranty**			9.5.3.4 The warranty on appliance would begin post successful acceptance and software post successful installation	we request that warranty for 3 year shall commence either from the date of installation or on completion of 30 days from date of delivery, whichever is earlier.	Bidder to comply with RFP terms
53	**Generic**	**Order cancellation**			12.17 Order Cancellation/Termination of Contract 12.17.1 The Bank reserves its right to cancel its entire/unexecuted part of the PO at any time by assigning appropriate reasons and recover expenditure incurred by the Bank in addition to recovery of liquidated damages in terms of contract, in the event of one or more of the following conditions 12.17.3 In such case Bank shall serve the notice of termination to the Bidder at least 30 days prior, of its intention to terminate services	Bank may terminate the contract for reasons to be recorded in writing by 90 days written termination notice/ Cure period to the Bidder. In case of termination of the contract, Bank shall be liable to pay the bidder all the dues (for the goods delivered or services rendered, cost incurred, or irrevocable committed to)payable till the effective date of termination.	Bidder to comply with RFP terms
54	**Generic**	**MTTR**			8.3 Mean Time To Restore (MTTR) for the Bidder 8.3.1 The bidders response time shall be less than 1 hour and the MTTR shall be less than 2 hours. Time specified above is from the time of lodging the complaint or intimation to the bidder	//////////////////2 hr for rectification is too less , please take MS team input on the MTTR	Bidder to comply with RFP terms
55	**Generic**	**Project timelines**			Project Timelines: Installation :Within 8 weeks from date of PO acceptance Implementation, Policy configurations,Acceptance testing and Go live:Within 4 months from date of PO acceptance	//////////////////Please take MS input on timelines	Bidder to comply with RFP terms
56	**Technical**	**Annexure 2**	**1.3**	52	Appliance should support a total of 3600 concurrent users. The same appliance system should be 100 % scalable over the next 5 years.	The appliance sizing is based on concurrent users, however the licenseing is based on total number of users. Please confirm wheather the proposal is required for 3600 users or 10939 users.	Refer to RFP-Addendum Item 4
57	**Technical**	**Annexure 2**	**1.4**	52	The solution should support NAT64, DNS64 & DHCPv6, IPV6 traffic, NTP server time synchronisation	NAT64/DNS54 & DHCPV6 are typically UTM/Firewall capabilities and are not provided by any Gartner Leaders or Challengers for Web Security. Request Bank to remove this point.	Refer to RFP-Addendum Item 5
58	**Technical**	**Annexure 2**	**2.15**	52	The solution should have visibility for cloud applications and shadow IT application usage	The visibility of cloud applications is not enough unless solution can block high risk and unauthorized cloud applications. We suggest Bank to revise it as: The solution should have visibility for cloud applications and shadow IT application usage alongwith the risks associated and also provide controls to block any/all cloud applications as per the requirement from the Bank	Refer to RFP-Addendum Item 6
59	**Technical**	**Annexure 2**	**2.15**		The solution should have visibility for cloud applications and shadow IT application usage	We support cloud applications , but Shadow IT application usage is a CASB feature	Refer to RFP-Addendum Item 6

60	**Technical**	**Annexure 2**	**2.2**		The proposed solution should support to provide real time data identifiers to detect and prevent sensitive information getting stolen by malware through web channel. Solution should have pre-built signatures to detect information leaks through malware.	The information leaks identification is a DLP solution use case. Web gateway can identify the destinations if the data is getting uploaded to a malware web category site.	Refer to RFP-Addendum Item 7
61	**Technical**	**Annexure 2**	**2.21**	53	The solution should be able to scan files, folders, databases and prevent the content from being sent over outbound web channel. The solution should have ability to provide geolocation awareness for security incidents	This will be a partial control unless key DLP features like Fingerprinting/ Machine Learning/Optical Character Recognition is included in proposed solution (as it was in Canara Bank SWG RFP). We suggest bank to revise it as: The solution should be able to scan files, folders, databases and prevent the content from being sent over outbound web channel. The solution should have ability to provide geolocation awareness for security incidents. The solution should support key DLP capabilities like Built in Template for Aadhar Card/PAN Card, Indian IT Act/Credit Cards, File/Database Fingerprinting, Machine Learning and Optical Character Recognition (To identify text in image files)	Bidder to comply with RFP terms
62	**Technical**	**Annexure 2**	**2.21**		The solution should be able to scan files, folders, databases and prevent the content from being sent over outbound web channel. The solution should have ability to provide geolocation awareness for security incidents	We don't support database files, IF it is related to the data protection, then it is a DLP solution use case.	Bidder to comply with RFP terms
63	**Technical**	**Annexure 2**	**2.39**	53	Solution should be able to restrict Users to download certain amount of data, for example a user can be restricted to use not more than 2 GB data during a time interval (parameterization)	Different solutions addresses the bandwidth management in different ways so we request Bank to revise it as: Solution should be able to restrict users/groups based on time/schedule/quota etc. to manage bandwidth effectively	Refer to RFP-Addendum Item 8
64	**Technical**	**Annexure 2**	**2.4**		The appliance should have the option to configure multiple IP addresses or a pool in the public facing interface of the proxy. Also there should be option to change the public IP address of the appliance for accessing a particular domain or IP addresses. The usefulness of this feature is when proxy servers IP address is getting blacklisted from other organizations.	Configuring of pool of ip for an interface is a Firewall Feature. Web gateway can be configured with any public IP which is routable and Multiple egress IPs can be selectively used based on rules.	Yes. This is called source NAT with Dynamic IP and Port (DIPP).
65	**Technical**	**Annexure 2**	**2.44**	53	The appliance should have provisions to restrict bandwidth per User.	Different solutions addresses the bandwidth management in different ways so we request Bank to revise it as: Solution should be able to restrict users/groups based on time/schedule/quota etc. to manage bandwidth effectively	Refer to RFP-Addendum Item 8
66	**Technical**	**Annexure 2**	**3.14**		The appliance should be capable of nullifying the malware/virus and should be able to stop the spreading of the same to other endpoints in the network. Solution should be able to identify the origin of the event and must take remedy for the issue immediately.	Stopping the spread of malware to other endpoints in the network is a Endpoint /EDR Feature.	Refer to RFP-Addendum Item 14
67	**Technical**	**Annexure 2**	**3.17**		The on-premises device should be able to work with existing 3rd party gateway antivirus of the bank	Need More Details on the current antivirus	Would be shared with the successful bidder
68	**Technical**	**Annexure 2**	**3.19**	**53**	Antimalware and antivirus engine should be different from the existing antivirus used by customer	Please provide current antivirus vendor name which is deployed at bank	Would be shared with the successful bidder

69	**Technical**	**Annexure 2**	**3.20**		The solution should be capable of integrating with on premises Sandboxing solution of the same OEM	Need More Details on the current Sandboxing solution	Refer to RFP-Addendum Item 13
70	**Technical**	**Annexure 2**	**3.22**		Solution shall provide forensic evidence on the infections activity within the network as follow: Event timestamp, network events in sequence, packet capture of suspicious communication, malware behaviors, malware type, severity, source and destination of attack	Repeated point 3.8 (Forensic evidence on the infections activity is a IPS/sandboxing/SIEM feature. Web gateway will be able to provide malware type, severity, source and destination of attack ONLY for further analysis.)	Refer to RFP-Addendum Item 9
71	**Technical**	**Annexure 2**	**3.4**		c) POP3, POP3S	POP3 & POP3S is an email protocol, Proxy is for TCP protocol	Refer to RFP-Addendum Item 14
72	**Technical**	**Annexure 2**	**3.5**		d) IMAP, IMAPS	IMAP, IMAPS is an email protocol, Proxy is for TCP protocol.	Refer to RFP-Addendum Item 14
73	**Technical**	**Annexure 2**	**3.7**	53	The solution should have Anti-APT features and should be able to integrate with Sandbox to detect and mitigate unknown threats and advanced threats	Please provide Sandbox vendor to check compatibility	Refer to RFP-Addendum Item 13
74	**Technical**	**Annexure 2**	**3.8**		Solution shall provide forensic evidence on the infections activity within the network as follow: Event timestamp, network events in sequence, packet capture of suspicious communication, malware behaviors, malware type, severity, source and destination of attack	Forensic evidence on the infections activity is a IPS/sandboxing/SIEM feature. Web gateway will be able to provide malware type, severity, source and destination of attack ONLY for further analysis.	Refer to RFP-Addendum Item 9
75	**Technical**	**Annexure 2**	**4.11**	54	The appliance when deployed in in-line mode should support bypass mode in case of appliance failure i.e. traffic flow should not break. Also there should be some indication to know whether bypass mode is active or not.	This is not a proxy capability and typically supported by the likes of UTM/WANOP devices. We request bank to remove this point.	Refer to RFP-Addendum Item 14
76	**Technical**	**Annexure 2**	**4.3**	54	The proposed solution shall be able to support various form of user Authentication methods simultaneously, including: Local Database entries	Local Database Entries will be OEM Specific, we request Bank to remove this point or make as optional.	Refer to RFP-Addendum Item 10
77	**Technical**	**Annexure 2**	**4.9**	54	The authentication should be done every time a user access web through the appliance after defined idle time. The appliance should timeout user if the connection is left idle for a certain amount of time. The solution should provide option to exclude the idle time for selected users or IP address groups and to set different range of idle time out period for different groups.	With microsoft sso (Kerberos/NTLM/ADFS etc.) in use, the timeout itself will not come in to picture till the machine is logged in to the domain. Further selective Idle timeout will be OEM specific, we request Bank to revise the point as: The authentication should be done every time a user access web through the appliance after defined idle time. The appliance should timeout user if the connection is left idle for a certain amount of time. The solution should provide option to exclude the idle time for selected users or IP address groups.	Refer to RFP-Addendum Item 11

78	**Technical**	**Annexure 2**	**5.1**	54	System should allow administrator to prevent sensitive data from leaving the network. Administrator should be able to define sensitive data patterns, and data matching these patterns that should be blocked and/or logged when passing through the unit.	This will be a partial control unless key DLP features like Fingerprinting/ Machine Learning/Optical Character Recognition is included in proposed solution (as it was in Canara Bank SWG RFP). We suggest bank to revise it as: The solution should be able to scan files, folders, databases and prevent the content from being sent over outbound web channel. The solution should have ability to provide geolocation awareness for security incidents. The solution should support key DLP capabilities like Built in Template for Aadhar Card/PAN Card, Indian IT Act/Credit Cards, File/Database Fingerprinting, Machine Learning and Optical Character Recognition (To identify text in image files)	Bidder to comply with RFP terms
79	**Technical**	**Annexure 2**	**5.4**		The solution should be able to detect data theft even if the malware sends the data through image files	Detection of data theft in a image format is a OCR functionality in DLP solution	Refer to RFP-Addendum Item 14
80	**Technical**	**Annexure 2**	**8.8**	**55**	The centralized management should be provided without the support of additional hardware/server (preferably) and if any additional devices required for the management of solution, it should be mentioned clearly	it is recommended to use centetrlized management server sepertly from the proxy appliance. Can we propose additional devices in the Bill of Material ?	Bidder is requitred to propose a solution on HA mode with dual identical management console on high availabiliy. Bidder is allowed to propose the mangement console within the SWG hardware or separately in the different hardware connected over network.
81	**Technical**	**Annexure 2**	**8.9**	55	Appliance shall support role-based administration such as Administrator, Entry user, Verification user and Read-only access user. The administrator should have the privilege to verify the pending modifications done from entry user.	Pending modifications validatation/approval will be OEM specific. We request Bank to revise the point as: Appliance shall support role-based administration such as Administrator, Entry user, Verification user and Read-only access user. The administrator should have the privilege to verify the changes/modifications done from entry user.	Bidder to comply with RFP terms
82	**Technical**	**Annexure 2**	**9.1**	55	The appliance should have complete and perpetual license for all the features required Web security solution, like Web filtering, Content inspection & control, Antivirus, reporting etc.	We request to revise it as: The appliance should have complete and perpetual/sunscription license for all the features required Web security solution, like Web filtering, Content inspection & control, Antivirus, reporting etc.	Bidder to comply with RFP terms
83	**Technical**	**Annexure 2**	**3.1, 3.2, 3.3, 3.4, 3.5, 3.6**	53	Should be able to block, allow or monitor only using AV signatures and file blocking based on policy or based on authenticated user groups with configurable selection of the following services: a) HTTP, HTTPS b) SMTP, SMTPS c) POP3, POP3S d) IMAP, IMAPS e) FTP, FTPS	SMTP/SMTPS/POP3/POP3S/IMAP/IMAPS/FTPS scanning is a UTM feature, and is not covered by any leading Web Security solutions including any Gartner Leader or Challenger. We request Bank to remove these points and cover only HTTP/ HTTPS/FTP.	Refer to RFP-Addendum Item 12
84	**Technical**	**Annexure 2**	**2.24**	53	The proposed solution should be a Fast Web Proxy and should support HTTP, FTP and HTTPS proxy.	Bidder recommends, not to use the HTTP & FTP ports being non secure ports.	Bidder to comply with RFP terms
85	**Technical**	**Annexure 2**	**5.2**	53	Solution should have web DLP functionality. Data Leakage prevention should prevent critical, sensitive and proprietary data from being leaked outside Bank`s secured network using web as channel.	Please share the definition parameters for Critical, sensistive & proprietary Data	Would be shared with the successful bidder

86	**Technical**	**Annexure 2**	**2.16**	52	The solution should perform HTTPS traffic deep packet inspection (SSL/TLS based).	Please share the details of protocols which shall be supported by the WSG appliances.	Bidder to comply with RFP terms
87	**Technical**	**Annexure 2**	**10.5**	53	All the regulatory compliance regarding web security solution should be adhered in the proposed solution.	Please share the details of Regulatory Requirements which shall be adhere by the solution.	This would be an ongoing activity based on changes made from time to time
88	**Technical**	**Annexure 2**	**2.21**	53	The solution should be able to scan files, folders, databases and prevent the content from being sent over outbound web channel. The solution should have ability to provide geolocation awareness for security incidents	Please share the qualification criteria for security incidents	Would be shared with the successful bidder
89	**Technical**	**Annexure 2**	**2.20**		The proposed solution should support to provide real time data identifiers to detect and prevent sensitive information getting stolen by malware through web channel. Solution should have pre-built signatures to detect information leaks through malware.	Please share the qualification criteria for sensitive information of Bank for adoption prospective.	Would be shared with the successful bidder
90	**Technical**	**Annexure 2**	**3.8**	53	Solution shall provide forensic evidence on the infections activity within the network as follow: Event timestamp, network events in sequence, packet capture of suspicious communication, malware behaviors, malware type, severity,source and destination of attack	What is the time period for which Forensic evidence on infection activity are anticipated	Refer to RFP Annexure 02 - clause 7.2. Solution should support exporting of data in standard readable format like csv, txt, xls etc as and when required by Bank.
91	**Technical**	**Annexure 2**	2.21	53	The solution should be able to scan files, folders, databases and prevent the content from being sent over outbound web channel. The solution should have ability to provide geolocation awareness for security incidents	Scanning of the data in database with respect to the data protection, it is a DLP solution functionality specification, we request bank to remove this specification in the RFP.	Bidder to comply with RFP terms
92	**Technical**	**Annexure 2**	2.4	53	The appliance should have the option to configure multiple IP addresses or a pool in the public facing interface of the proxy. Also there should be option to change the public IP address of the appliance for accessing a particular domain or IP addresses. The usefulness of this feature is when proxy servers IP address is getting blacklisted from other organizations.	Configuring of pool of IP for an interface is a Firewall feature. Web gateway can be configured with any public IP which is routable and Multiple egress IPs can be selectively used based on rules. Please change the specification as below: "The appliance should have the option to configure multiple IP addresses or a pool in the public facing interface or should have option to configure using the rules of the proxy. Also there should be option to change the public IP address of the appliance for accessing a particular domain or IP addresses or should have option to configure using the rules of the proxy. The usefulness of this feature is when proxy servers IP address is getting blacklisted from other organizations."	This is called source NAT with Dynamic IP and Port (DIPP).
93	**Technical**	**Annexure 2**	3.17	53	The on-premises device should be able to work with existing 3rd party gateway antivirus of the bank	We would need more details on the current antivirus for the integration, request bank to modify this point	Would be shared with the successful bidder