Request for Information

For

Secure Web Gateway Solution

RFI Reference: SBIL/DIG/2023/SWG

RFI Release Date: 16th March 2023
Last Date of Submission: 7th April 2023

Response to be sent to
Swgrfp.sbilife.co.in

Table of Contents

Introduction

SBI Life Insurance ('SBI Life' / 'The Company'), one of the most trusted life insurance companies in India, was incorporated in October 2000 and is registered with the Insurance Regulatory and Development Authority of India (IRDAI) in March 2001.

Serving millions of families across India, SBI Life's diverse range of products caters to individuals as well as group customers through Protection, Pension, Savings and Health solutions.

Driven by 'Customer-First' approach, SBI Life places great emphasis on maintaining world class operating efficiency and providing hassle-free claim settlement experience to its customers by following high ethical standards of service. Additionally, SBI Life is committed to enhance digital experiences for its customers, distributors and employees alike.

SBI Life strives to make insurance accessible to all, with its extensive presence across the country through its 990 offices, 20,286 employees, a large and productive individual agent network of about 193,635 agents, 59 corporate agents and 14 bancassurance partners with more than 38,000 partner branches, 129 brokers and other insurance marketing firms.

In addition to doing what's right for the customers, the company is also committed to provide a healthy and flexible work environment for its employees to excel personally and professionally.

SBI Life strongly encourages a culture of giving back to the society and has made substantial contribution in the areas of child education, healthcare, disaster relief and environmental upgrade. In 2021-22, the Company touched over 2 lakh direct beneficiaries through various CSR interventions.

Listed on the Bombay Stock Exchange ('BSE') and the National Stock Exchange ('NSE'), the company has an authorized capital of ₹20.0 billion and a paid-up capital of ₹10.0 billion. The AuM is ₹2,999.9 billion.

Primary business and technical goals

SBI Life has embarked on a Digital Transformation journey to achieve the following objectives

- Enhance customer and partner Experience
- Improve employee satisfaction and productivity
- Achieve operations excellence
- Expand and grow business

- Compliance to all regulatory and corporate policies

Business Requirement

1. Provide safe internet access to users from advance threats.
2. Protect from Legal liability, Security Risk and reduce Network Bandwidth Loss and Productivity Loss.
3. Should provide in-built multiple malware engine for scanning at network level.
4. Should have option for critical data protection over web channel with license upgrade.
5. Seamless Integration with existing security devices and tools present and future tools planned for procurement.
6. Granular filtering of URL on user basis.
7. Single appliance for enterprise class proxy & caching with URL filtering.
8. Real time content classification, categorization and security scanning on real time basis inbuilt with proxy solution
9. SSL decryption inbuilt with proxy solution to scan HTTPS & tunnel protocol traffic.
10. Advance application control inbuilt with proxy solution like ultrasurf, tor etc. • Granular control on social networking sites.
11. Single policy and management console for network users and roaming users as well.
12. Should provide high availability for business resiliency.
13. Should have a centralized and powerful management which should enable BL to deploy, view and control secure web gateway through a single console. Able to manage and deploy policy through single management console.

IT Plays a very critical role in achieving the Digital Transformation objectives supporting the business by providing high-availability and high-performance systems and applications, enhance user and customer experience by providing the easy-to-use applications and simple tools.

In summary, SBI Life IT Team is looking for and would ensure Always-ON, secured connectivity and access to tools and applications for users, partners, and customers.

SBI Life would like to build a future ready Digital Foundation infrastructure to seamlessly adopt cloud and SaaS applications soon. In this regard SBI Life is planning to migrate the Traditional based On-Premise Proxy Solution with Enterprise class Secure Web gateway Solution consisting of SSE (Secure Service Edge) Framework which can take care of Modern Threats while accessing the Internet.

The SSE Framework would consist of the following

a) ZTNA: - Zero Trust Network Access
b) CASB: - Cloud Access Security Broker
c) RBI: - Remote Browser Isolation
d) FAAS: - Firewall as a Service

Strategic related IT projects

SBI Life Insurance in achieving its goal in improving customer and user experience, optimize IT operations and lower total cost of ownership by transforming the traditional Proxy Solution to Enterprise Class Secure Web Gateway Solution.

The Objectives:

- Need #1: Secure Access to Internet Website with comprehensive Threat Protection
- Need #2: Improve IT Operations / User Experience while browsing Internet Websites
- Need #3: Lower Total Cost of Ownership
- Need #4: Should be able to integrate with existing IT Networking & Security infrastructure solution related to Data Governance and Data Protection.
- Need #5: Enable secured Internet connectivity for adoption of Cloud services

Goals

- Deployment of Enterprise Secure Web Gateway Solution with SSE in Hybrid Mode for SBI Life

Section 1 - Solution Management, Architecture and Analyst Evaluation Requirements

Sr.	Requirement	Response
1	Share brief information on all the solution components and products.	
2	Briefly describe key differentiators of your Secure Web Gateway solution.	
3	How is your solution rated in the 2022 Gartner Magic Quadrant or Forrester for Secure Service Edge?	
4	How is your solution rated in other analyst evaluations?	
5	Can you provide an architectural diagram(s) for your solution?	
6	Describe your high-availability architecture for the solution? HA in DC and co-existence in DC & DR.	
7	How long has your Web Proxy solution been available in the marketplace?	
8	Describe the licensing models for on-premise SWG, hybrid mode.	

	Would there be additional licenses required in case customer decides to move web proxy solution from on-premise to cloud?	
9	Customer references in Indian BFSI	
10	Solution should support leading Cloud Service Providers in India & should support micro-services type architecture OR any other Platform Agnostic Solution.	

Section 2 -Secure Web Access

Sr.	Requirement	Response
1	List the sandbox vendors with which you integrate.	
2	Describe at a high-level how your solution supports secure web, Secure Service Edge and cloud usage	
3	Describe hybrid deployment options	
4	Describe how the solution can allow for blocking of malicious sites by URL?	
5	How does your Secure Web Proxy solution protect roaming users from zero-day malware?	
6	Apply SSL inspection for both on-premise and roaming users?	
7	Describe how your solution deals with untrusted certificates, such as allowing or blocking such sites.	
8	What modes do you support to steer traffic to your proxy?	
9	Describe the ability of your solution to access databases of known-good and known malicious URLs. Also, describe what options you offer for actions such as SSL Intercept, block, trace of hostname/IP address, etc., based on the value of the risk score.	
10	How many URL categories are provided/supported in your SSE solution? How many categories can a URL be categorized into? Describe how many policy decisions are made for a URL that fits both allow and deny actions based on different categories?	

11	Do customers have the ability to apply their own classification(s) to specific websites?	
12	SWG should support traffic decryption. With over 80% of global internet traffic encrypted using SSL/Transport Layer Security (TLS), including a great deal of traffic that is largely undesirable.	
13	Are external URL filtering lists supported in your product?	
14	Describe the ability of your solution to set policies per (1) pre-defined and custom categories such as File Sharing or Gambling and (2) or by blacklisting or whitelisting individual URLs.	
15	Do you maintain specific categories for security and malicious sites including: ▪ Known Bot-Nets ▪ Known command and control servers ▪ Compromised/malicious sites ▪ Crypto mining ▪ Hacking sites ▪ Malware call-Home ▪ Malware distribution point Phishing/Fraud ▪ Ad Fraud ▪ Spam sites ▪ Spyware & questionable software ▪ Peer to peer ▪ Dynamic DNS ▪ DNS tunneling VPN	
16	Describe what reporting functions your solution provides to report on traffic distribution and bandwidth statistics for traffic running through the SWG, including specific information on user or group usage patterns.	
17	What protocols are supported and what are limitations/constraints with the level of support (such as TLS1.3, HTTP/3, DoH, IPv6)?	
18	Is the traffic between the client and the proxy encrypted?	
19	Does the solution utilize signature-based and signature-less malware detection?	
20	List the DLP vendors with which your solution can integrate.	

21	Seamless integration with Active Directory	
22	Seamless user experience irrespective of user location (Home/Office) without changes in endpoint setting	
23	Does the solution require Proxy PAC file to be configured for Internal and External Network?	
24	Does the solution seamlessly work with Endpoint devices like Windows and Mac, and Mobile Devices like Android and Mac?	
25	Do you own the SSL technology, or is it licensed from an OEM provider?	
26	Does the Solution integrate with Wi-Fi Networks to provide Seamless Proxy Integration	
27	Can you customize block pages for the enterprise? What branding options are possible?	
28	List the 3rd party Reputation Servers the solution integrated for Website reputation and Risk Scoring.	
29	Does the solution have Local POP in India and Data that resides in India policy? Also does your Solution ensure that 100% of data resides in India with Traffic steering only within Indian Territory	
30	Does your solution’s Tenant Restrictions support both personal and corporate credentials with appropriate policies? Can users configure and apply policies appropriately depending on whether a given user is using corporate or personal credentials on a managed device?	

Section 3 -Private Access / Zero Trust Network Access (ZTNA)

Sr.	Requirement	Response
1	Describe at a high-level how your ZTNA solution enables enterprises to connect and secure remote workers.	
2	Describe how your SSE solution supports key ZTNA principles? And CASB solution and security Policies	
3	How does your ZTNA solution replace network-level VPN access with application-	

	level, context-aware, identity-based access ZTNA?	
4	At a high-level, how does your SSE solution support adaptive access control in an enterprise?	
5	Explain how your ZTNA solution can enrich activity reporting.	
6	Provide bullet points that demonstrate how your ZTNA solution improves the experience for an organization employee.	
7	In terms of enterprise architecture, can your ZTNA solution potentially reduce IT and networking costs?	
8	How is your ZTNA solution deployed?	
9	What differentiates your ZTNA solution?	
10	How can DLP policies be applied for ZTNA traffic?	
11	How can threat protection be applied to ZNTA traffic?	
12	What is the preferred approach for supporting off-network systems including Windows, Mac, Linux, iOS, and Android?	
13	What capabilities does your SSE solution have around geolocation of sources and destinations? Can you define rules/policies around geolocation information?	
14	Can the solution integrate with SD-WAN technologies? Please detail which vendors are available for integrations.	
15	What authentication methods are supported by the solution.	
16	How are your Cryptographic Keys Managed	
17	Provide Understanding of CASB Architecture and all Key Security Policies of CASB like (Authentication, Crypto, Credential Mapping, tokenization, logging, SSO, Alerting, Authorized / Unauthorized cloud usage visibility, Device Profiling, Malware Detection / Prevention.	
18	What all components are been offered within CASB like (Firewalls, Authentication, WAF, DLP etc.)	

Section 4 -SSE Platform, Enterprise Application Integration, Product Security, and Certifications

Sr.	Requirement	Response
1	Integration with SIEMs?	
2	Does the management console of your SSE solution provide configuration/policy versioning? Is there an option to roll back to a specific previous version? Can you selectively rollback selected changes?	
3	Does your solution allow custom reporting in addition to the default reporting templates?	
4	Integration with On-Premise DLP solution	
5	Does the solution has undergone OSWAP top 10 Vulnerability scanning and does it have a certificate for security vendor like Cert-IN etc.	
6	Does the solution ensure that the Product is bug free from Known malwares, Viruses etc.	

Section 5 -Service & Support

Sr.	Requirement	Response
1	Are professional services available with 24*7 Support?	
2	What is your implementation methodology?	
3	Is customer support included in the pricing? Are there varying tiers of customer support that we can purchase?	
4	Do you provide Customer Support days and hours of operation? Is support 24x7x365 for all customers?	
5	Can support tickets be logged via web and phone?	
6	Describe the methods of communication (e.g., web portal, email notifications, etc.) that you provide for real-time status of your service, product updates, scheduled maintenance, security advisories, etc.	

Eligibility Criteria

1. The participant must be a legal entity, capable of entering into an agreement on its own capacity or through its partner.
2. If a company, the participant must be incorporated in India. If a partnership firm, it must have been registered in India.
3. The participant must be the authorized System Integrator (SI) of OEM.
4. Minimum Annual Turnover should be ` 100 Crores in each of the preceding three financial years.
5. The participant should be a profit-making entity. Bidder should be profitable in 2 years out of 3 preceding financial years.
6. The participant should have offices / point of presence across India. It should be able to demonstrate its service and quick resolution capability.
7. The participant should produce a declaration that it has not been blacklisted by any public sector organization.
8. The OEM should have 24 X 7 X 365 Technical Assistance Center in India for customer support.
9. In case any component of proposed solution fails to meet or scale to the requirement in terms of sizing, specifications, features, throughput etc. mentioned in this RFI / RFP document, the bidder will have to upgrade or replace the components with no commercial implications to SBI Life.
10. Supplied equipment should not be declared End-of-Support by the vendor while proposing in RA and should not go out of sale post supply for minimum 7 years.
11. Incase supplied equipment goes out of End of sale then rollover model should be supplied with the same price during tenure of price validity.
12. SLA should be executed with SI but OEM should provide proof or certification that SI have uploaded order to OEM with desired SLA terms. It is mandatory requirement to process invoices.
13. The selected bidder would be required to submit a performance Bank Guarantee (PBG) with validity of 3 years to the SBI Life for an amount equivalent to 10% of order value within 30 days of purchase order issue date.

General Terms & Conditions

1. OEM must produce at least three references of successful implementation of SWG (Secure Web Gateway and SSE (Secure Service Edge) deployment in Enterprises in India / Global. Out of the above 3 deployments, at least one successful deployment should be from India Banking, Finance and Insurance segment.
2. At least one deployment of more than 15000 users.
3. Solution should integrate seamlessly with existing architecture without missing on any of the existing network features/functionalities.
4. Solution should posses all necessary capabilities of the current solution and should offer more, to cater to Sbilife Insurance needs and requirement for Unified end user experience.

Non-Disclosure Agreement

This Nondisclosure Agreement ("NDA") is made and entered into this <Current Date>

BY AND BETWEEN

SBI Life Insurance Co Ltd., a company incorporated under the laws of Indian Companies Act 1956 and having its registered office at Natraj, M.V. Road, Western Express Highway Junction,

Andheri (East) Mumbai- 400069

AND

<Partner Address>

SBI Life Insurance Co Ltd. and <Partner Company and Partner Address>**.,** shall be individually referred to herein as a "Party" and collectively as the "Parties".

WHEREAS, the Parties propose to exchange certain proprietary information, concerning Technically and commercially detailed information regarding their respective products & service offerings, organization, decision processes.

s, technical infrastructure, working processes and delegation of responsibilities, project management and planning methods, reports, plans and status including but not limited to technical manuals, specifications, product features, customer list, specialization, documents, financial statements and business/development plans ("Proprietary Information").

WHEREAS, each Party agrees to receive the proprietary information or other information from the other party and treat all such information as confidential information and such information will be treated as confidential

NOW, THEREFORE, in consideration of the recitals set forth above and the covenants set forth herein, the Parties agree that:

1. Recipient agrees to hold all Confidential Information received from the Disclosing Party in confidence. Recipient will use such Confidential Information only for the purpose of business arrangements between the Parties; restrict disclosure of such Confidential Information to its employees and employees of its affiliated companies with a need to know and inform such employees of the obligations assumed herein. Recipient will not disclose such Confidential Information to any third party without the prior written approval of the Disclosing Party.

2. The Confidential Information means information which may be in any form including but not limited to oral, written or printed information or Information in electronic form, data, studies, consultants'

reports, trade secrets, proformas and other financial and trade/commercial information, computer models and programs, contracts, plant designs and configurations, plant performance data or other material of any kind or nature in whatever form. Wherever, information is given orally, within 48 hours, the receiving party should receive the information in writing along with the confidentiality statement from the other party.

3. Without the prior written consent of the other party or except as otherwise provided herein, either party will not: (i) distribute or disclose to any other person any of the Confidential Information; (ii) permit any other person to have access to the Confidential Information; (iii) use the Confidential Information for any purpose other than the Permitted Use ; or (iv) disclose to any other person (A) that discussions, investigations or negotiations are taking place concerning a possible transaction between the Parties, or (B) the terms, conditions, status or other facts regarding a possible transaction between the Parties, or (C) that either party has received Confidential Information from the other Party. Notwithstanding the above, either party may disclose the Confidential Information, and portions thereof to its directors, officers, employees and representatives of its advisors (collectively, "Representatives") who need to know such Confidential Information for the purpose of evaluating a possible transaction between the Parties. It is understood that the parties will inform their respective Representatives of the confidential nature of the Confidential Information and will require its Representatives to be bound by this Agreement and not to disclose the Confidential Information to any other person. The parties agree to be responsible for any breach of this Agreement by their respective Representatives.

4. Recipient agrees to protect the Confidential Information received from the Disclosing Party with at least the same degree of care as it normally exercises to protect its own proprietary information of a similar nature. Recipient agrees to promptly inform the Disclosing Party of any unauthorised disclosure of the Disclosing Party’s Confidential Information.

5. The Recipient shall ensure that their employees will not disclose any information of the disclosing party even after they cease to be the employees of the recipient. The recipient party shall ensure this by their own internal agreements

6. Confidential Information does not include information that either party can reasonably prove, falls within any of the following: (i) information that either is legally in either party’s possession or publicly available to either party prior to the disclosure of such information hereunder; (ii) information that, subsequent to its disclosure hereunder, becomes publicly available to either party without any violation of this Agreement by either party; (iii) information that becomes legally available to either party on a non-confidential basis from any third party, the disclosure of which to either party does not, to either party’s knowledge, violate any contractual or legal obligation such third party has to either party with respect to such information ; (iv) information that is independently acquired or developed by either party which can be evidenced by written records; or (v) information that is explicitly approved for release by written authorization of either party.

7. In the event that either party is required by law in any judicial or governmental proceeding or otherwise to disclose any Confidential Information, the disclosing party will give the other party prompt written notice of such request so that the other party may seek a protective order or appropriate remedy. If, in the absence of a protective order, disclosing party determines, upon the advice of counsel, that it is required to disclose such Confidential Information, it may disclose such Confidential Information only to the extent compelled to do so; provided, however, that the disclosing party gives the other party written notice of the portion of Confidential Information to be disclosed as far in advance of the disclosure as is practicable and uses its best efforts, at its own expense, to obtain assurances that confidential treatment will be accorded to such Confidential Information.

8. No license expressed or implied in the Confidential Information is granted to either party other than to use the information in the manner as is permitted in writing by the parties.

9. Both parties agree that Confidential Information is and shall at all times remain the property of the owning party. Both parties acknowledge that the Confidential Information is confidential and material to the interests, business and affairs of the other party and that the disclosure thereof (other than as permitted under this Agreement) would be detrimental to the interests, business and affairs of the other party. No use of such Confidential Information is permitted except as otherwise provided herein and no grant under any of the party's intellectual property rights is hereby given or intended, including any license (implied or otherwise). All information shall remain the property of the Disclosing Party and shall be returned upon written request or upon the Recipient's determination that it no longer has a need for such information.

10. No license to the Recipient, under any trade secret or any other intellectual property right, is either granted or implied by the disclosure of information to the Recipient. None of the information which may be disclosed or exchanged by the Parties shall constitute any representation, warranty, assurance, guarantee, or inducement by either Party to the other of any kind, and in particular, with respect to the non-infringement of trademarks, patents, copyrights, mask work rights, or any other intellectual property rights, or other rights of third persons or of either Party.

11. There are no warranties expressed or implied by this Agreement. Without limiting the foregoing, neither party makes any representations nor extend any warranties, express or implied, as to the adequacy or accuracy of Confidential Proprietary Information or any other information or data related thereto, or with respect to the use thereof by Recipient.

12. Neither this NDA nor the disclosure or receipt of information from either Party to the other Party, shall constitute or imply any promise or intention to pursue any business opportunity described in the Confidential Information or make any purchase of products or services by either Party or its affiliated companies or any commitment by either Party or its affiliated companies with respect to the present or future transaction between the parties.

13. Either party shall not modify or erase the logos, trademarks etc., of the other party or any third party present on the Confidential Information. Neither party shall use or display the logos, trademarks etc., of the other party in any advertisement, press etc., without the prior written consent of the other party.

14. Upon the request of a party, the other party, will within 7 days of receipt of such request, return or destroy all Confidential Information and any notes, correspondence, analyses, documents or other records containing Confidential Information, including all copies thereof, then in the possession of either party or its Representatives and shall certify the fact of having destroyed the Confidential Information in writing to the other party. Such return, however, does not abrogate the continuing obligations of both parties under this Agreement.

15. In case of any cyber security incident/ data breach, which involves SBIL data, the recipient of SBIL data shall be accountable and liable for all the consequences arising out of such cyber security incident / data breach, in accordance with the prevailing laws and regulations.

16. Both parties agree and acknowledge that monetary damages would not be a sufficient remedy for a breach of this Agreement and that the both parties shall be entitled to seek from a court of appropriate jurisdiction a decree of specific performance or any other injunctive relief as a remedy in equity for any such breach of this Agreement. Any remedy shall not be deemed to be exclusive or all-inclusive and shall be in addition to any and all other remedies which may be available to the either party in law or equity.

17. Confidential Information provided to one party does not and is not intended to represent an inducement by the other party or a commitment by the Disclosing Party to enter into any business relationship with the Recipient or with any other entity. If the parties desire to pursue business opportunities, the parties will execute a separate written agreement to govern such business relationship.

18. The Parties agree that during the existence of the term of this NDA and for a period of five years thereafter, neither Party shall solicit directly or indirectly the employees of the other Party.

19. Each Party agrees that all of its obligations undertaken herein as the Recipient of confidential information shall be for the term of five (5) years and shall survive for 3 years after the termination of this NDA.

20. This NDA constitutes the entire understanding between the Parties hereto as to the information and merges all prior discussions between them relating thereto.

21. No amendment or modification of this NDA shall be valid or binding on the Parties unless made in writing and signed on behalf of each of the Parties by their respective authorised officers or representatives.

22. The Parties understand and agree that no failure or delay by either Party in exercising any right, power or privilege hereunder shall operate as a waiver thereof, nor shall any single or partial exercise thereof preclude any other or further exercise thereof or the exercise of any right, power or privilege hereunder.

23. This Agreement shall be governed and construed in accordance with the laws of India

24. In the event that any of the provisions of this Agreement shall be held by a court or other tribunal of competent jurisdiction to be unenforceable, the remaining portions hereof shall remain in full force and effect.

25. Both parties agree not to assign this Agreement or any interest herein without express prior written consent of the other party.

26. Nothing in this agreement and no action taken by the Parties pursuant to this agreement shall constitute, or be deemed to constitute, a partnership, association, joint venture or other co-operative entity or arrangement. This Agreement is entered into by the Parties on a Principal-to-Principal basis and no other meaning can be assigned in interpreting any of the terms contained herein.

27. Any dispute or claim arising out of or in connection herewith, or the breach, termination or invalidity thereof, shall be settled by arbitration in accordance with the provisions of Procedure of the Indian Arbitration & Conciliation Act, 1996. The arbitration tribunal shall be composed of a sole arbitrator, and the Parties shall appoint such arbitrator with mutual consent the place of arbitration shall be Mumbai, India and the arbitration proceedings shall take place in the English language.

IN WITNESS WHEREOF, the parties have caused this Agreement to be executed as of the date set forth above.

SBI Life Insurance Co. Ltd.	**<Partner Company Name>**
By:	By:
Name:	Name:
Title:	Title:
Date:	Date: