Section-E: SCOPE OF WORK

The scope of work includes understanding the requirement, customizing and providing the deployment architecture of proposed solution. Supply, install and commission the respective appliances at LIC data centers. Configure the appliance for High availability, Tune up the appliances with LIC Security requirement in line with the IRDAI guidelines; document the solution, Train candidates nominated by LIC. This is not an all-inclusive list. The Bidder is expected to provide the end to end solution and vendor is expected to absorb any other cost of material / services if any not particularly listed below.

General

- Supply of Security devices/products with provision for version upgrades/patches
- Installation and implementation of the products/devices as per the security architecture design; this will include device rules / device policy definition and enforcement on the Security devices proposed in this RFP.
- Vendor has to act as technical-advisor to LIC for gateway security products and related systems by way of evaluation, demonstration, etc. as and when required by LIC. Vendor has to submit findings/reports to LIC and give suggestions/recommendations. Necessary resources (including Level-3 support) have to be deployed by vendor for technical assistance and submit the detailed documentations etc. No additional cost will be payable by LIC for such things.
- Identifies potential security risks, helping LIC to take appropriate, corrective action
- Design, implement, and keep record & controls and migration to IPv6 as and when required by LIC without any additional cost to LIC.
- In case there is a cost incurred to LIC due the wrong BoM/Specification/feature-set of security equipment/device/appliance at any location, the same will have to be replaced by vendor at no extra cost to LIC.
- Prepare test-plan, migration plan and rollback strategies
- Monitoring, onsite support and offsite support
- The successful bidder shall co-ordinate and co-operate with the other vendors appointed by the LIC so that the work shall proceed smoothly without any delay and to the satisfaction of LIC.
- No extra claim shall be entertained on account of all/part of any job redone on account of bidder's negligence which results into damages/losses during execution of the job. Also, any component(s) required to deliver the solution after release of Purchase Order shall have to be provided by the successful bidder. All such cost shall be borne by the bidder.
- The vendor has to provide complete escalation matrix which should be updated and sent to LIC as and when there is a change.
- The bidder has to perform an OEM audit (involving both the OEMs) immediately after the deployment of the solution. The OEM audit has to provide a detailed report on the hardening and best practices to be adopted. Rule reviews to remove all unused, covered, shadow rules etc. should be conducted. All aspects of technical specifications should be verified for the implementation. IS Audit requirements as per the IRDAI/other regulatory guidelines should be complied with. The audit should also cover compliance with any legal, regulatory or industry requirements.
- After the first OEM audit, immediately after deployment the bidder has to perform a half yearly OEM audit and provide a detailed report on the hardening and best practices to be adopted. Rule reviews to remove all unused, covered, shadow rules etc. should be conducted. All aspects of technical specifications should be verified for the implementation. IS Audit requirements as per the IRDAI/other regulatory guidelines should be complied with. The audit should also cover compliance with any legal, regulatory or industry requirements and should provide recommendations on the latest security posture to be adopted in view of the evolving threat landscape.
- The OEM Audit report should be made available within seven days of conducting the OEM Audit. The System Integrator has to ensure that all the shortcomings pointed out in the OEM Audit report are rectified and all the recommendations are complied with within fifteen working days.
- The identity of the Auditors conducting the OEM audit has to be suitably established , through the names and other attributes such as Aadhar Card Details/Passport Details, mail-id etc. provided on the letterhead of the OEM .
- The Bidder has to formulate the BCP processes in line with the IRDAI guidelines and conduct DR Drill

twice a year. The DR drill conducted has to be evaluated by a third party (CERT-In empanelled).

1.1. Details of Work

- Total solution will cover supply, decommissioning of the existing solution, installation, implementation, testing, training, supporting the firewall, management and reporting appliance during warranty period. This will also include installation, configuration and maintenance of associated appliances like routers, switches, Link load balancers etc. which may be provided by LIC.
- Prepare HLD and LLD in consultation with OEM and LIC for rollout. The design should be OEM certified.
- Design and document a Project implementation plan with significant milestones marked on it.
- The selected bidder needs to configure firewall appliance in High Availability (HA) mode (Active-standby) and configure management and reporting appliance with applicable features set as deemed fit to address the LIC Network gateway security requirement.
- The successful bidder need to install all the associated equipment needed to complete the job as per the technical specification described in this tender.
- Bidder needs to study existing Client, Server, LAN& WAN network environment of LIC and suggest suitable changes for deployment of proposed solution.
- The firewall solution needs to be integrated with LIC's existing Local Area Network, Wide Area Network, Server and Security infrastructure etc. The selected bidder needs to work closely with the LIC for preparation and configuration of Firewall policies.
- The installation will include proper mounting, labeling, tagging of all the equipment and provide network and power connections.
- The bidder shall be responsible to provide within scope of work all facilities like labor, transportation, tool Kits, testing equipment etc. which is necessary for successful deployment of solution.
- Transportation to & fro, lodging and boarding of manpower shall be in vendors scope. (Present Locations are Vile-Parle (S.V. Road, Mumbai 400054), Yogakshema (Nariman Point, Mumbai 400021), IDC (Prabhadevi, Mumbai) and Bengaluru.

1.2. Design and Architecture

Bidder has to architect the solution deployment after understanding the following details:

- Understanding the Network in terms of Network, Server and Security appliances, LAN, WAN & Internet Links and segments etc.
- Prepare the designs and implement the solution in line with the IRDA guidelines and ISO27001:2013 standards as modified from time to time.
- Study of LIC's existing security environment and guidelines and recommend best practices to implement and roll out the same.
- Study of our present architecture at Data centers.
- To suggest plan for network integration of all the four Data centers.
- Design of Network gateway Security Architecture.
- Design should ensure that communication to the critical server zones must pass through NGFW at each location.
- Depending on the business requirement, dynamic routing may be implemented in Firewalls.
- Design and document the IP addressing Schema (IPv4 as well as IPv6) in accordance with requirement of LIC and the government agencies/regulators.
- Design and document the ACLs and VLAN schema for the network along with LIC team.
- Bidder needs to prepare a detailed execution plan. The complete documented plan must be submitted to LIC with supported designs and drawings (if any) within 6 weeks of placing the order. The actual execution will start only after approval of plan by LIC officials.
- The plan shall include information related to required downtime, changes to existing architecture, deployment schedule etc. The installation of the equipment shall be done as a planned activity on a date & time of approved deployment schedule.

1.3. Inspection and Acceptance Procedure

- Physical Inspection and preliminary testing of the product/s shall be done at LIC, in the presence of representatives of the supplier and will comprise of the following:

a) Physical verification of equipment as per the supply contract.
b) Physical inspection of the equipment for any physical damage.
c) "Power on self-test" to ascertain that no product/s is dead on arrival.
d) Physical verification of Licenses, Software media, technical documentation as per purchase order.
e) Registering the Hardware & Software License with OEM for validation and desired technical support.

1.4. Basic Installation of Hardware and Software

Bidder has to perform following jobs for completing the above mentioned activity:

- Mounting physical devices onto racks as required.
- Powering on the physical devices & running Hardware Diagnostics.
- Installing the required OS and Applications on Physical Hardware.
- Configuring IP address and default gateway etc. on all devices
- Check L2 & L3 connectivity on network using "ping & trace route" commands
- Installing License if any on respective appliances.
- Enabling of features and functionality on respective Appliances for Application control and detection, IPS, Anti-spyware, Botnet detection, Data Content Filtering, VPN, SSL, Management, Logging and Reporting etc.
- Configure Firewall Appliances in HA mode (either in Active-Active or Active-Standby as specified by LIC while execution)
- Integration with AD (Active Directory) to facilitate user identification.
- Configure all automated updates for all security features by NGFW.
- Configuration of update and upgrades as and when the latest version is released.
- Configuring backup Schedule of Firewall, Management, Logging and Reporting appliance.
- Check for Failover between appliances used for Firewalling.
- Policies to be set to prevent DOS/DDOS attacks.
- The successful bidder has to migrate the data from the existing firewall to the new firewall being installed. The successful data migration done has to be verified and certified by a third party (CERT-In empaneled).
- Monthly security life cycle review in the form of executive summary report providing threat landscape in LIC.

1.5. Deploying and Fine Tuning of Firewall Appliances

- Migrate the existing security policies to new firewall after reviewing the same in consultation with LIC.
- Design and document the Firewall policies and rules to be configured on the Perimeter and Core Firewalls.
- Creating and applying default policies after analyzing traffic pattern for monitoring purpose.
- Modifying and Fine-tuning existing default policies for better traffic control
- Configuring IPS module on Firewall Appliances in detect mode with default / recommended profile for analysis
- Configuring and fine tuning the DNS security features.
- Configuring and fine tuning the APT features.
- Configure Objects and rules on the Firewall management console.
- Block critical and high categories attacks/viruses and alert for all other categories.
- Test connectivity to and from the various network zones configured on the Firewall.
- Creating customized IPS profile based on the outcome of detect mode analysis
- Configuring firewall with enabled feature sets mentioned in 1.4 above.
- Configuring QoS to enhance the response for identified services
- Configuring user authentication through LDAP for device administration and VPN access.
- Setting up basic system health monitoring and log analysis through Management and Reporting appliance.
- Vendor has to do end-to-end configuration of network gateway security devices, designing, implementation and customization as per best practices and LIC's requirements. The vendor will ensure seamless integration of its equipment for functioning of existing as well as future gateway security appliances.

1.6. Deploying Management, Logging & Reporting Appliance

Configuration of Management, Logging and Reporting Server/Appliance would involve following tasks:

- Configuring Management and reporting appliances for capturing performance and availability of Firewall devices.

- Enable capturing of logs, log retention period and mechanism for archiving logs.
- Review of firewall policies every month to identify the unwanted and overlapping rules.
- Creating Out-of-the-box reports and customized reports templates based on the needs of LIC.
- Scheduling of backup for device used for Management purpose.
- Checking up of restoration of Management hardware from backup.
- Configure Incident based alert mechanism supported by appliance like Visual Alerts, e-mail & SMS etc.

1.7. Documentation

- All the documents shall be supplied in properly bound volumes of A4 size sheets.
- Three sets of hardcopies as applicable and one softcopy on CD shall be supplied as final document.
- Documents for high level design, detailed design, configuration of individual features set on various appliances, general testing, scenario based fail-over testing, Standard Operating Procedure in accordance with the IRDAI guidelines (exhaustive including backup, Procedures, Quality Assurance/Quality Control etc.), best practices etc. shall form the complete set for fulfilling the documentation criteria.
- The SOPs have to be reviewed quarterly and changes, if any, have to be incorporated. In either case (with changes or without changes) the updated version of SOP in the latest quarter has to be prepared and submitted.
- Vendor shall also submit Delivery and Installation Report, Warranty certificates, License Copies for all the items supplied along with the supplies.
- Installation report should contain the part numbers of all the components supplied by the selected bidders.

1.8. Training

Bidder shall train specified LIC employees, not exceeding 12 in number, for operational Management of the system at LIC premises. Training shall be provided on each of the following modules to specified LIC personnel. Training shall be provided at no additional cost to LIC through OEM approved authorized agencies/faculties.

- Pre-Implementation: Provide training to the LIC personnel/ Onsite and offsite support team on the product architecture, functionality and the design for each solution under the scope of this RFP.
- Post Implementation: Provide hands-on training to the LIC personnel/ Onsite and offsite support team on Firewall operations, alert monitoring, policy configuration for all solutions etc.
- Documentation and knowledge transfer after each patch/version update.
- The bidder and OEM approved authorized agencies/faculties are required to provide training jointly as per the below table for people nominated by the LIC for each solution specified in the scope of work.
- The bidder and OEM approved authorized agencies/faculties are required to provide ad-hoc trainings to the LIC staff as required by LIC, to acquaint them with the latest features and functionalities of the solutions for minimum of one day. LIC has the right to exercise this training option at its discretion.
- Training cost shall be inclusive of certification of at least two participants.
- The bidder is required to provide all trainees with detailed training material and 3 additional copies to the LIC for each solution as per the scope of work of the LIC. This training material should cover installation, operation, integration, maintenance, troubleshooting and other necessary areas for each solution.
- All out of pocket expenses related to training shall be borne by the selected bidder.

Solution	**Pre-Implementation (Days)**	**Post-implementation (Days)**
Firewall	2	5

The detailed training documents should be given to the training participants. The detailed theory & hands-on training should be imparted by the OEM authorized personnel at LIC premises.

The training facilities shall be made available by LIC, the Bidder will have to ensure that training is imparted in a professional manner through certified and experienced personnel (other than on-site Personnel) and proper course-ware is given to every person attending the training.

1.9 Acceptance by LIC

- Decommissioning of the existing solution.
- Degaussing of the existing solution before taking the decommissioned solution for buyback.

- Certification from third party that the decommissioned firewall does not contain any data/configuration.
- The Bidder has to ensure that a competent team of OEM conducts an audit of the implemented solution in order to confirm that the implementation and configuration has been done as per OEM best practices and design, IRDAI IS Audit guidelines. It is suitable to deliver 99.5% uptime. All the securities features sought in the technical specifications and the scope of work have been implemented.
- The Goods supplied by the Bidder should meet the technical specifications envisaged in this tender document.
- A comprehensive "Acceptance Test Plan" document, containing various aspects of the 'Acceptance Test' to demonstrate all the features of the proposed Solution, shall be submitted by the bidder.
- Scenario based Acceptance Test shall be carried out jointly by the representatives of LIC and the Bidder after the Installation.
- Acceptance tests should explicitly Demonstrate High Availability (HA) features, automatic failover features, demonstrate Inbound and outbound filtering, blocking of ports as per policies, intrusion prevention and AntiBot features etc.
- Appliances will be considered to have been commissioned when all services as described in this tender document are able to run smoothly over the network. Mere installation of appliances with out-of-the box features will not constitute as commissioning of the proposed solution.
- The final acceptance will be provided by LIC after verifying all aspects as mentioned in the document have been delivered to satisfaction.

LIC has the right to the following aspects:

- Access Control (logical, physical, administrative etc.) of all security products has to be shared with LIC officials, but vendor should implement in such a way that accountability can be fixed,
- To ascertain the effectiveness and efficiency of the resources deployed for facility management (L1 & L2 Personnel)
- To ascertain the effectiveness and efficiency of the resources deployed for offsite support.
- The vendor will do the necessary changes in the security infrastructure as per the changing business needs without charging any cost to LIC

1.10 Performance and Support Assurance

The System Integrator and OEM must provide the following performance assurances on the NGFW solution:

- During the immediate post deployment demonstration of the NGFW solution in the live environment, the system integrator and OEM must demonstrate that the Memory and CPU average utilization of the firewall doesn't exceed 50% of the total memory and CPU capacity during 30 days in live production environment i.e., after acceptance. In case this requirement is not met, then the OEM and System Integrator must replace the Firewall with a higher capacity box to meet this requirement without any additional cost implication to the LIC.
- The OEM and System Integrator must assure that all types of support including warranty, security, upgrade and maintenance support for hardware, software and any other component shall be available throughout the contract period. In case any of the components of the solution is declared end of support by the OEM, the same shall be replaced with an equivalent or higher component without any cost implication to the LIC. Solution/upgrade for any newly emerged threat/vulnerabilities must be provided without any additional cost to LIC.
- Stage of Product life cycle: The Software and engineering support for all the equipment/devices offered in the Total Solution must be available till the end of Contract Period (Taking into account the implementation period from the date of purchase order). During SW and Engineering support the OEMs would continue to develop, repair, maintain, and test the product software including operating system and release appropriate bug-fixes/patches/updates. Documentary evidence for "Stage of product Life Cycle" must be from the information/documents available in public domain.

The firewall shall be able to provide reporting and MIS as per the detailed specifications. In case, OEM is not able to provide the same, third party software/hardware may be used. For any such third-party tool and/or tool of the OEM/s the respective OEM of the NGFW will be responsible and accountable for smooth, efficient and effective performance of such tools during the entire contract period

1.11 RACI Matrix

Below Table depicts desired RACI (Responsible-R, Accountable-A, Consulted-C, Informed-I) matrix for proposed engagement which is non-exhaustive. The successful bidder must submit comprehensive RACI for proposed services in a similar way in their response to RFP.

Activity	SI	OEM	LIC
Plan, Design, Implementation	R,A, Implementation	R,A	C, I
Device Monitoring Best Practices Audit- Identify existing monitoring parameters, recommended monitoring practices, and formulate a corrective action plan.	A	R	C,I
Device and Performance Monitoring	R,A	C	I
Monitoring Tool/Software availability and Support	R,A	R,A	C, I
Service Request Handling	**R,A**	**C**	**I**
Incident Detection and Notification	R,A	C	I
Incident Troubleshooting	A	R	C,I
Incident Communication Updates	R,A	R,A	C,I
Incident Escalation	R,A	R,A	C,I
Incident Closure- Restoration	R,A	R,A	C,I
Problem Management- Root Cause Analysis (24 hours)	R,A	R,A	C,I
Configuration Change Plan	R,A	C	I
Impact Analysis and Change Validation	R,C	R,A	I
Change Approval	A	C,I	R
Change- Method of Procedure	R	A	C,I
Change Execution	R,A	A	C,I
Change Communication	R,A	C	I
Impact analysis of Rules , CRF for NGFW	R,A	C	I
QOS for NGFW	R,A	A	C,I
Third Party and/or OEM's own additional tool for NGFW management and performance analysis	R,A	R,A	C,I
Proactive Software Risk Assessment/ Software Selection	R,C	R,A	I
Software Implementation	R	A	C,I
Software Security Vulnerability Assessment	R	A	C,I
Configuration Audit, Best Practices	R,A	R,A	C,I
Configuration Remediation	R,A	C	I
Capacity Audit and Benchmarking	A	R	C,I

Performance Audit	R,A	R	C,I
Capacity and Performance Monitoring	R,A	C	I
Inventory Management	R,A	C	I
License Management	R,A	C	I
Reporting	R,A	C	I
SLA Performance	R,A	R,A	C,I
SLA Reporting	R,A	C	I
Service Delivery Review and Governance	R,A	R,A	C,I
First Information report (FIR) on incident (4 hrs)	R,A	R,A	C,I
Business Continuity Management	R,A	R,A	C,I
Proactive Threat Assessment	R,A	R,A	C,I

Compliance with IS Security Policy:

The Vendor shall have to comply with LIC's IT & IS Security policy in key concern areas relevant to the RFP, details of which will be shared with the finally selected Bidder. Some of the key areas are as under:

i. Responsibilities for data and application privacy and confidentiality;
ii. Responsibilities on system and software access control and administration;
iii. Custodial responsibilities for data, software, hardware and other assets of LIC being managed by or assigned to the Vendor;
iv. Physical Security of the facilities;
v. Physical and logical separation from other customers of the Vendor;
vi. Incident response and reporting procedures;
vii. Password Policy;
viii. Access management Policy;
ix. Acceptable usage Policy (Authentication and Identity Management, Authorization and access control);
x. Data Encryption / Protection requirements of LIC;
xi. Cyber Security Policy;
xii. Auditing;
xiii. In general, confidentiality, integrity and availability, non-repudiation, authenticity, privacy of data/information must be ensured;
xiv. Responsibilities in carrying out background verification of personnel deployed from vendor side regularly and submit the report as and when needed by LIC;

Right to Audit

i. It is agreed by and between the parties that the Service Provider shall get itself annually audited by external empaneled Auditors appointed by LIC/ inspecting official from the IRDAI or any regulatory authority, covering the risk parameters finalized by LIC/ such auditors in the areas of products (IT hardware/ software) and services etc. provided to LIC and the vendor shall submit such certification by such Auditors to LIC. The vendor and or his / their outsourced agents /sub – contractors (if allowed by LIC) shall facilitate the same. LIC can make its expert assessment on the efficiency and effectiveness of the security, control, risk management, governance system and process created by the Service Provider. The Service Provider shall, whenever required by such Auditors, furnish all relevant information, records/data to them. All costs for such audit shall be borne by LIC.

ii. Where any deficiency has been observed during audit of the Service Provider on the risk parameters finalized by LIC or in the certification submitted by the Auditors, it is agreed upon by the Service Provider that it shall correct/ resolve the same at the earliest and shall provide all necessary documents related to resolution thereof and the auditor shall further certify in respect of resolution of the deficiencies. It is also

agreed that the Service Provider shall provide certification of the auditor to LIC regarding compliance of the observations made by the auditors covering the respective risk parameters against which such deficiencies observed. All costs for such audit shall be borne by the service provider/vendor.

iii. Service Provider further agrees that whenever required by LIC, it will furnish all relevant information, records/data to such auditors and/or inspecting officials of the LIC/ IRDAI and or any regulatory authority required for conducting the audit. LIC reserves the right to call and/or retain for any relevant material information / reports including audit or review reports undertaken by the Service Provider (e.g., financial, internal control and security reviews) & findings made on the Service Provider in conjunction with the services provided to LIC.