Sl. No.	Page No	Clause No.	Description of Terms / Headings / Query Segments	Clause [in brief] of RFP requiring clarificartion[s]	Deviations / Recommendations (Bidder's view)	Clarifications/Modifications	LIC's Response
1	Tech	1.11	Perimeter DC	The Proposed hardware & product model should be available from OEM at least for 1 year and should not be end of support for next 7 years.	Appliance refresh cycle practice in Industry is 5-7 years and even LIC is doing a refesh after 5 years. OEM should be taking ownership and delivering commitment on the same. This looks like latest applinaces from the OEM should not qualify.	Please be guided by the RFP	No Change
2	Tech	1.2	Perimeter DC	The proposed application security solution must be in the Leader's quadrant in the Gartner "Magic Quadrant of Enterprise Network Firewall" as per the latest available report	There are only two firewall vendors in leader quandrant of Gartner's report. We request LIC to include "Challenger" quadrant also which will ultimately provide price benefit to LIC because of more competition.	Please be guided by the RFP	No Change
3	Tech	1.2	Perimeter DC	The proposed application security solution must be in the Leader's quadrant in the Gartner "Magic Quadrant of Enterprise Network Firewall" as per the latest available report	Contradictory Statement - Application Security is specific function to achieve Secure Application Delivary/accessibility. Asking for Gartner's Quadrant Leader for Enterprise Firewall doesnot make sence	Please be guided by the RFP	No Change
4	Tech	1.2	Perimeter DC	The proposed application security solution must be in the Leader's quadrant in the Gartner "Magic Quadrant of Enterprise Network Firewall" as per the latest available report	Achieving the Leader's Level is purely on Business Volume of OEM in respective Segment. Hence we propose as per Suggestion. And also propose to add an option with Gartner's Quadrant or NSSLabs Recommendation with above 96% of rating for Security Value Map in latest report	Please be guided by the RFP	No Change
5	Tech	1.6	Perimeter DC	Security effectiveness should be certified by NSS and should be more than 98.5%	Why Specifically 98.5%?	LIC would like to be the closest to highest possible security effectivenss as per NSS labs report	No Change
6	Tech	1.6	Perimeter DC	Security effectiveness should be certified by NSS and should be more than 98.5%	Clause should allow atleast three OEMs present in INDIA with sales, service & support.	Please be guided by the RFP	No Change
7	Tech	1.6	Perimeter DC	Security effectiveness should be certified by NSS and should be more than 98.5%	LIC should consider Security Effectiveness of NSS NGFW test. Since this tender is for NGFW only NGFW test conducted conduted by NSS in 2016 should be considered and not any other.	We are open to any security test report by NSS where OEM has achieved 98.5% security effectiveness	No Change
8	Tech	1.7	Perimeter DC	The Proposed solution should allow policy creation for application identification,user identification,host profile,threat prevention etc in single rule and not at multiple locations.	From the Security and Managemnet consideration different OEM bulid framework of Next Genertaion Access Control and Threat Prevention along with segegration of duties and not necessarily in a Single rule.	Accepted	Proposed solution vendor should support creation of Unified Policy in Single Dashboard. Policy creation for Access Controls including Application Identification, User Identification, Host and Threat Prevention within same dashboard window
9	Tech	1.8	Perimeter DC	The Proposed solution must have minimum of 100GB HDD for storing logs etc.	Current Security Solution deployed alreday have 160 GB HDD and now with NGFW and Threat Prevetion Features there will more data hence we recommend to have at least 250GB or more.	Please be guided by the RFP	No Change
10	Tech	1.8	Perimeter DC	The Proposed solution must have minimum of 100GB HDD for storing logs etc.	**Suggestion** - We strongy recommend LIC to go for SSD based HDD. There are many advantage of SSD HDD - 1 - SSD HDD improves the over all life cycle of the product as there is no moving part involved. 2 - SSD HDD improves the mean time between failure (MTBF) since SSD drives are more sturdy as compare to SATA / SAS drive which has moving part and prone to failure more often. 3 - SSD HDD provide far better perofrmance (read/write) as compare to SATA / SAS.	LIC would prefer SSD HDD. However its not mandatory. This is minimum requirement and bidder is free to propose anything higher or better.	No Change
11	Tech	1.9	Perimeter DC	The proposed appliance must have at least 12 x 1G Copper Ports from day one. It should be expandable to total 16 x 1G ports and 4 x 10G ports.	**Query** - 1-Please clarify if 16 x 1G & 4 x 10G required from day one. 2- if all ports need to be Data / Production Ports exclusive of management + sync ports. 3- If 16x1G & 4x10G to be achieved simultaneously.	Clarification Issued	The proposed appliance must have at least 12 x 1G Copper Ports from day one. It should be expandable to total 16 x 1G ports and 4 x 10G ports. Management,sync,HA etc ports should be additional

12	Tech	2.1	Perimeter DC	The proposed solution must provide minimum 5 Gbps of throughput (i.e. it should support 5 Gbps of ingress traffic and 5 Gbps of outgress traffic simultaneously) with all security features enabled including Application Control + IPS + Anti Spyware + Anti Bot + Antivirus + DDoS along with all signature turned ON. The performance must be based on HTTP traffic and not UDP. The claim has to be supported by publicly available documents	Query - Please clarify what form of supported document will be acceptable by LIC.	Clarification Issued	LIC is looking for threat prevention throughput as published by each OEM. For Checkpoint it is published as "NGTP - Next Generation Threat Prevention" & For Palo Alto it is published as "Threat Prevention". LIC has observed that the data sheets of various models mentions the throughput with desired features in the specifications. LIC is looking for similar reference document from OEM to support the claim.Such documents should be dated prior to the RFP publishing date. Any document other than publicly available documents will be acceptable at the sole discretion of LIC.
13	Tech	2.1	Perimeter DC	The Proposed solution must provide minimum 5 Gbps of throughput (ie it should support 5 Gbps ingress traffic and 5 Gbps of outgress traffic simultaneously) with all security features enabled including applicaiton control + Antispyware+AntiBot+Antivirus+DDOS along with all signatures turned on.The performance must be based on HTTP traffic and not UDP.The claim has to be supported by publicly documents.	Most of the OEM publishes Performnace numbers based on Generic Test Results also know as Ideal Testing Conditions and this performnace data will be availbale with these vendors on public documnent. Certain vendors publishes testing results based on Industry Production Blend of traffic. There is a specific ask from LIC and none of the vendor publishes the performance numbers based on the criteria as asked by LIC. There is no benchmarking defined by LIC for Perfromnace testing and its generic. Vendor needs to test mentioed security controls along with IPS, AB, AV and IPS with DDOS Signatures as aksed by LIC and certify the same. This needs to be done considering the signature details as asked in the specification for apple to apple comparision. Also SSL needs to be delivered as per clause 6.6 as none of the vendor published SSL traffic seperately in Public documents.	Clarification Issued	LIC is looking for threat prevention throughput as published by each OEM. For Checkpoint it is published as "NGTP - Next Generation Threat Prevention" & For Palo Alto it is published as "Threat Prevention". LIC has observed that the data sheets of various models mentions the throughput with desired features in the specifications. LIC is looking for similar reference document from OEM to support the claim.Such documents should be dated prior to the RFP publishing date. Any document other than publicly available documents will be acceptable at the sole discretion of LIC.
14	Tech	2.3	Perimeter DC	10,00,000 Concurrent Sessions	Mismatch in Concurrent Sessions and New sessions figures	Please be guided by the RFP	No Change
15	Tech	2.3	Perimeter DC	10,00,000 Concurrent Sessions	Concurrent Sessions shall be maximum 10x to New sessions. [As defined for PerimeterDR-NDR & CoreDR-NDR firewalls]	Please be guided by the RFP	No Change
16	Tech	2.5	Perimeter DC	The proposed solution must be able to handle minimum 2 Gbps IPSEC VPN throughput.	Need to know parameters on arriving this throughput	LIC is planning to provide VPN connectivity to remote branches and such branches opening in future which have been used as parameters to arrive at this throughput.	No Change
17	Tech	2.6	Perimeter DC	The proposed solution must support minimum 2000 Site to Site IPSEC VPN tunnels. The proposed solution must support minimum 4000 Remote / Mobile Access VPN Connections. All licenses needs to be provisioned from day one.	Query - Please clarify if 4000 Remote / Mobile access VPN connections are required client - to - site VPN connections	Yes, 4000 client to site VPN connections are required .	No Change
18	Tech	3.1	Perimeter DC	The proposed solution must support, Port mirroring, Transparent, Layer 2 , Layer 3 mode providing flexibile deployment.	Query - Please clarify if all these / more than one mode required simultaneously.	LIC would prefer all modes simultaneosuly.However its not mandatory	No Change
19	Tech	3.13	Perimeter DC	The Proposed solution must have virtual router capabilites that supports all L3 capabilities.The proposed solution must have IPv6 static routing support even for virtual routers.	Need to know the use case and business need of Virtual Routers as there are no virtual firewalls.	Deleted	Deleted
20	Tech	3.15	Perimeter DC	The OEM must provide 24 X 7 X 365 highest level of technical support. The OEM must provide the dedicated login credentials to LIC with highest level permissions to search knowledge base, downloading of the patches, documents and to manage the device. LIC should be able to raise tickets directly to OEMs	Query - Please clarify if LIC is looking for Direct Enterprise Support from OEM	Clarification Issued	In addition to what is stated in the specification LIC wants enterprise and direct OEM support/contract .Its should be the highest level of support which could come under different names for different OEMS.

21	Tech	4.13	Perimeter DC	The proposed solution must support user-identification over wireless by integrating with wireless controller.	Need to know the use case and expectation on integration.	LIC is currently using Wireless infrastructre from Cisco. LIC would like to integrate Cisco Wireless solution with NGFW for user-identification.	No Change
22	Tech	4.13	Perimeter DC	The proposed solution must support user-identification over wireless by integrating with wireless controller.	Query - Please clarify what Wireless infrastructure LIC is using?	LIC is currently using Wireless infrastructre from Cisco. LIC would like to integrate Cisco Wireless solution with NGFW for user-identification.	No Change
23	Tech	4.2	Perimeter DC	user Identification using all of the following technologies AD, LDAP, 2FA, eDirectory, Radius, Kerberos, client certificate from day one..	We would like to know if LIC is using eDirectory and need to know usecase of having user integration with the same.Incase,OEM doesnot support eDirectory integration.	Modifed	The proposed solution should provide seamless AD Integration with multiple deployment options like Clientless, Captive Portal or Identity Agent on endpoints. The proposed solution must support authentication services for user-identification using all of the following technologies AD, LDAP, 2FA, Radius, Kerberos, Client Certificate from day one. The Solution must include User Directory capabilities to integrate over LDAP.
24	Tech	4.4	Perimeter DC	The Proposed solution must support policy based forwarding based zone,applications,network source/destination address,user or user group.	Certain vendors address Zone Based concepts via different ways currently and not necessarily as Zone Based Naming. Zone Based Naming conventions are part of next release	It is acceptable to LIC if bidder is providing necessary support document that this feature will be available in the next release in the near future. Please clearly mention time line, cost & any other relevant details.	No Change
25	Tech	4.6	Perimeter DC	The proposed solution must be able to handle unknown/unidentified applications e.g. alert, block or allow	Query - Please clarify what does LIC mean by unknown / un-identified applications.	LIC would like to implement positive security model and hence would like to identify all applications traversing in the network currently. It may require to create some custom app signature to identify home made applications. Over and above these application if any traffic is traversing across LIC network, can be classified as Unknown traffic. LIC would like to have complete control of such traffic and should able to Alert, Block or Allow such traffic as per LIC needs.	No Change
26	Tech	4.7	Perimeter DC	The proposed solution must be able to create custom application signatures and categories based on LIC environment.	Query - Please clarify if LIC want to create custom application for HTTP / HTTPS / TCP based application. In case of HTTPS will LIC allow SSL Decryption?	LIC would like to create custom application signature for home grown applications. It may use HTTP, HTTPS, TCP, UDP etc for communication. NGFW must have capability to create application signature irrrespective of protocols used. It will be preferred if the signature can be creaetd for HTTPS traffic without decryption. LIC would like to keep choice with them to decypt traffic.	No Change
27	Tech	5.1	perimeter DC	The proposed solution must provide IPS, Antivirus, AntiBot & Spyware protection features form day one.Integrated IPS must have been tested NSS labs & secured recommended rating recently (last 2 years)	Integrated IPS is a part of NGFW and since LIC is considering NGFW solution hence need to consider NSS Report of NGFW. Should consider latest report only as NSS conducts multiple test every year and its not possible to participate in all the testing conducted by NSS.	Modifed	The proposed solution must provide IPS, Antivirus, AntiBot & Spyware protection features form day one.Integrated IPS must have been tested NSS labs & secured recommended rating in the last test in which it has particpated .
28	Tech	5.22	Perimeter DC	The proposed solution must provide flexibilty to detect and prevent Zero Day attacks.	Query - Please clarify is LIC is looking for Zero Day Prevention / APT solution. Typically it requires dynamic & behavioural analyses of unknown files in a control environment (sand boxing). Sand Boxing can be done over cloud - which will require LIC to send data over internet to OEM cloud hosted out side India. OR an on-premises device need to be deployed in addition to NGFW for sanndboxing.	Clarification Issued	It is clarified that "The proposed model should provide flexibility to integrate with on-premises sand boxing / APT solution to provide prevention against Zero Day Attacks in future"

29	Tech	5.24	Perimeter DC	Proposed Firewall shall integrate with dedicated Email Security Solution that shall detect & block Data leakage pertaining to Credit Card info from LIC Network	DLP Requirement very Generic - it shall be for Mail Traffic	No such specification .	No Change
30	Tech	5.24	Perimeter DC	Proposed Firewall shall integrate with dedicated Email Security Solution that shall detect & block Data leakage pertaining to Credit Card info from LIC Network	Specific Function not clearly defined, Perimeter firewall are PCI Compliant solution, web traffic can be handled for such requirement. Hence we proposed to add Email Protection as well through Dedicated Email Security Solution.	No such specification .	No Change
31	Tech	5.24	Perimeter DC	Solution must be able to provide Data leakage prevention - DLP capabilities to stop credit card & other important information leaving from LIC's network.All DLP related licenses need to be provided form day one	Need more info on DLP as why are we asking basic DLP features only and not more advanced like fingerprinting,watermarking, out of box DLP policies, supported file-types etc. DLP solution should focus on advance Data Prevention capabilities and not just Credit Card.	The minimum requirements for DLP have been mentioned in the specification. Bidder is free to propose additional features.	No Change
32	Tech	5.31	Perimeter DC	Monitor web communication for potential executable code,confirms the presence of executable codes and identify whether executable code is malicious.	Need to know the use case and LIC's expectation from the solution	LIC would like to detect any malicious payload / files traversing during web communication and provide prevention against it.	No Change
33	Tech	5.34	Perimeter DC	Threat events/protection exclusion rules can be created and view packet data directly from log entries with RAW Packets and if required can be sent to Wireshark for the analysis.	Query - Please clarify if LIC requires data packet capture on Firewall / Management device for security incident such as virus, spyware etc.	LIC desire to capture the raw packets on Firewall for any security event, rule, based on custom filter etc.	No Change
34	Tech	5.36	Perimeter DC	Customize security profiles for specifc set of Services including IPS etc	Are we setting up Server or Firewall[Typo mistake]	LIC would like to have the flexiblity to create custom security profiles for critical servers	No Change
35	Tech	5.36	Perimeter DC	Customize security profiles for specifc set of Services including IPS etc	It seems it's a typo mistake	LIC would like to have the flexiblity to create custom security profiles for critical servers	No Change
36	Tech	5.8	Perimeter DC	The proposed solutionmust support different actions in the policy such as deny,drop,reset client,reset server,reset both client and server	In case of action related to Detect, Prevent and Drop are considered Reset of Client and Server are not required hence not required.	Modifed	The proposed solution must support different actions in the policy such as alert/detect,prevent/deny,drop,packet capture
37	Tech	6.3	perimeter DC	The proposed solution must support decryption and inspection of SSL traffic in an outbound,inbound connection across any port.	Ned to know use case of SSL on any port.	LIC is running many application on non-generic TCP ports such as http is running on 8080 etc. Similalry https is also running on non-generic ports (other than 443). LIC would like to have the ability to detect SSL on such ports & decrypt it if desired.	No Change
38	Tech	6.5	Perimeter DC	The proposed solution must suppor on appliance per policy SSL and SSH decryption for both inbound and outbound traffic.	Need to know the use case of SSH decryption and impact incase,OEM doesnot support the feature.	Modifed	The proposed solution must support on appliance Per policy SSL decryption for both inbound and outbound traffic.Proposed solution should support identification and inspection of SSH traffic
39	Tech	6.6	perimeter DC	The SSL decryption throughput should be minimum 10% of the overall throughput as mentioned above.	What is the benchmarking to arrive at 10% of HTTPS Throughput when Industry SSL traffic is gorwing at the rate of more than 18%-20%.	The said performance is minimum requirement of LIC and bidder is free to propose higher throughput.	No Change
40	Tech	6.6	Perimeter DC	The SSL decryption throughput should be minimum 10% of the overall throughput as mentioned above.	Query - Please clarify if it needs to be minimum 500 Mbps.	Please be guided by the RFP	No Change
41	Tech	8.1	Perimeter DC	Dedicated management solution must be provided for management, logging and reporting. End to End infrastructure in this regards has to be provided by the vendor. Management and reporting solution is required at DC, DR. They should be in realtime sync	Query - Please clarify if bidder is proposing virtual management platform does it also need to include Server, OS etc.	Please be guided by the RFP	No Change
42	Tech	8.18	Perimeter DC	The management solution must have automated workflow feature to include management aproval for changes to be applied in firewall cofiguration.	Query - The foresaid feature is only available with one firewall vendor. Request LIC to kindly modify it to be more generic. It can be "The management solution must have third party integration capabilities with broader Eco System partner to achieve multiple functionalities inluding Firewall Chanage Management & Automation. Management solution must provide integration using API."	Deleted	

43	Tech	8.3	Perimeter DC	Solution should support minimum 6 TB of storage space for logs and reporting.	Query - Please clarify if storage is required with redundancy. Also if 6TB is pre-raid or post raid (usable storage).	Clarification Issued	Solution should support minimum 6 TB of usable storage space for logs and reporting along with RAID-5 redundancy.
44	Tech	3.14.5	Perimeter DC	Proposed firewall shall have Inbuilt Dual Hot Swappable Redundant Power Supply with Indian Standard compatible Power cords	Requirement is not clearly defined	No such specification .	No Change
45	Tech	3.14.5	Perimeter DC	Proposed firewall shall have Inbuilt Dual Hot Swappable Redundant Power Supply with Indian Standard compatible Power cords	Perimeter or Core Firewalls shall not rely on External Dual Power Supply. Using term for integrated will allow positioning of firewall with external dual power supplies. Hence we propose to amend more specifically defined requirement.	No such specification .	No Change
46	Tech	3.14.6	Perimeter DC	Dual (redundant) HDD	Query - Please clarify if HDD is SSD or SATA & What Redundancy / RAID type required.	Clarification Issued	LIC would prefer SSD but it is not mandatory. RAID should be RAID 1
47	Tech	8.1 & 3	Perimeter DC	The proposed Enterprise Grade Firewall integrate with External Logging and Reporting solution from same OEM. External Solution shall have at least 6TB of Storage space.	Log storage shall have multiple option external or Internal, but in DC setup external is prefered	Please be guided by the RFP	No Change
48	Tech	8.1 & 3	Perimeter DC	The proposed Enterprise Grade Firewall integrate with External Logging and Reporting solution from same OEM. External Solution shall have at least 6TB of Storage space.	Storage on appliance shall be used for Multiple configuration, Real time logs and Historical Logs the best practice is to have external Storage location. Dedicated Management Solution with logging and reporting capbilities is already part of requirement with 6TB of storage on Req.no. 8.1[please refer]	Please be guided by the RFP	No Change
49	Tech	1.11	Perimeter DR-NDR	The proposed hardware & product model should be available from OEM at least for last 1 year and should not be End of Support for next 7 years.	Appliance refresh cycle practice in Industry is 5-7 years and even LIC is doing a refesh after 5 years. OEM should be taking ownership and delivering commitment on the same. This looks like latest applinaces from the OEM should not qualify.	Please be guided by the RFP	No Change
50	Tech	1.2	Perimeter DR-NDR	The proposed application security solution must be in the Leader’s quadrant in the Gartner "Magic Quadrant for Enterprise Network Firewalls" as per the latest available report.	There are only two firewall vendors in leader quandrant of Gartner's report. We request LIC to include "Challenger" quadrant also which will ultimately provide price benefit to LIC because of more competition.	Please be guided by the RFP	No Change
51	Tech	1.2	Perimeter DR-NDR	The proposed application security solution must be in the Leader’s quadrant in the Gartner "Magic Quadrant for Enterprise Network Firewalls" as per the latest available report.	Contradictory Statement - Application Security is specific function to achieve Secure Application Delivary/accessibility. Asking for Gartner's Quadrant Leader for Enterprise Firewall doesnot make sence	Please be guided by the RFP	No Change
52	Tech	1.2	Perimeter DR-NDR	The proposed application security solution must be in the Leader’s quadrant in the Gartner "Magic Quadrant for Enterprise Network Firewalls" as per the latest available report.	Achieving the Leader's Level is purely on Business Volume of OEM in respective Segment. Hence we propose as per Suggestion. And also propose to add an option with Gartner's Quadrant or NSSLabs Recommendation with above 96% of rating for Security Value Map in latest report	Please be guided by the RFP	No Change
53	Tech	1.6	Perimeter DR-NDR	Security effectiveness should be certified by NSS and should be more than 98.5%	Why Specifically 98.5%?	LIC would like to be the closes to highest possible security effectivenss as per NSS labs report	No Change
54	Tech	1.6	Perimeter DR-NDR	Security effectiveness should be certified by NSS and should be more than 98.5%	Clause should allow atleast three OEMs present in INDIA with sales, service & support.	Please be guided by the RFP	No Change
55	Tech	1.6	Perimeter DR-NDR	Security effectiveness should be certified by NSS and should be more than 98.5%	LIC should consider Security Effectiveness of NSS NGFW test. Since this tender is for NGFW only NGFW test conducted conduted by NSS in 2016 should be considered and not any other.	We are open to any security test report by NSS where OEM has achieved 98.5% security effectiveness	No Change
56	Tech	1.7	Perimeter DR-NDR	The proposed solution should allow policy rule creation for application identification, user identification, host profile, threat prevention, etc in a single rule and not at multiple locations.	From the Security and Managemnet consideration different OEM bulid framework of Next Genertaion Access Control and Threat Prevention along with segegration of duties and not necessarily in a Single rule.	Accepted	Proposed solution vendor should support creation of Unified Policy in Single Dashboard. Policy creation for Access Controls including Application Identification, User Identification, Host and Threat Prevention within same dashboard window
57	Tech	1.8	Perimeter DR-NDR	The proposed solution must have minimum 100 GB HDD for storing logs etc.	Current Security Solution deployed alreday have 160 GB HDD and now with NGFW and Threat Prevetion Features there will more data hence we recommend to have at least 250GB or more.	Please be guided by the RFP	No Change

58	Tech	1.8	Perimeter DR-NDR	The proposed solution must have minimum 100 GB HDD for storing logs etc.	Log storage shall have multiple option external or Internal, but in DC setup external is prefered	Please be guided by the RFP	No Change
59	Tech	1.8	Perimeter DR-NDR	The proposed solution must have minimum 100 GB HDD for storing logs etc.	Storage on appliance shall be used for Multiple configuration, Real time logs and Historical Logs the best practice is to have external Storage location. Dedicated Management Solution with logging and reporting capbilities is already part of requirement with 6TB of storage on Req.no. 8.1[please refer]	Please be guided by the RFP	No Change
60	Tech	1.8	Perimeter DR-NDR	The proposed solution must have minimum 100 GB HDD for storing logs etc.	**Suggestion** - We strongy recommend LIC to go for SSD based HDD. There are many advantage of SSD HDD - 1 - SSD HDD improves the over all life cycle of the product as there is no moving part involved. 2 - SSD HDD improves the mean time between failure (MTBF) since SSD drives are more sturdy as compare to SATA / SAS drive which has moving part and prone to failure more often. 3 - SSD HDD provide far better perofrmance (read/write) as compare to SATA / SAS.	LIC would prefer SSD HDD. However its not mandatory. This is minimum requirement and bidder is free to propose anything higher or better.	No Change
61	Tech	1.9	Perimeter DR-NDR	The proposed appliance must have at least 12 x 1G Copper Ports from day one. It should be expandable to total 16 x 1G ports.	**Query** - 1-Please clarify if 16 x 1G required from day one. 2- if all ports need to be Data / Production Ports exclusive of management + sync ports.	Clarification Issued	The proposed appliance must have at least 12 x 1G Copper Ports from day one. It should be expandable to total 16 x 1G ports. Management,sync,HA etc ports should be additional
62	Tech	2.1	Perimeter DR-NDR	The proposed solution must provide minimum 2 Gbps of throughput (i.e. it should support 2 Gbps of ingress traffic and 2 Gbps of outgress traffic simultaneously) with all security features enabled including Application Control + IPS + Anti Spyware + Anti Bot + Antivirus + DDoS along with all signature turned ON. The performance must be based on HTTP traffic and not UDP. The claim has to be supported by publicly available documents	Most of the OEM publishes Performnace numbers based on Generic Test Results also know as Ideal Testing Conditions and this performnace data will be availbale with these vendors on public documnent. Certain vendors publishes testing results based on Industry Production Blend of traffic. There is a specific ask from LIC and none of the vendor publishes the performance numbers based on the criteria as asked by LIC. There is no benchmarking defined by LIC for Perfromnace testing and its generic. Vendor needs to test mentioed security controls along with IPS, AB, AV and IPS with DDOS Signatures as aksed by LIC and certify the same. This needs to be done considering the signature details as asked in the specification for apple to apple comparision. Also SSL needs to be delivered as per clause 6.6 as none of the vendor published SSL traffic seperately in Public documents.	Clarification Issued	LIC is looking for threat prevention throughput as published by each OEM. For Checkpoint it is published as "NGTP - Next Generation Threat Prevention" & For Palo Alto it is published as "Threat Prevention". LIC has observed that the data sheets of various models mentions the throughput with desired features in the specifications. LIC is looking for similar reference document from OEM to support the claim.Such documents should be dated prior to the RFP publishing date. Any document other than publicly available documents will be acceptable at the sole discretion of LIC.
63	Tech	2.1	Perimeter DR-NDR	The proposed solution must provide minimum 2 Gbps of throughput (i.e. it should support 2 Gbps of ingress traffic and 2 Gbps of outgress traffic simultaneously) with all security features enabled including Application Control + IPS + Anti Spyware + Anti Bot + Antivirus + DDoS along with all signature turned ON. The performance must be based on HTTP traffic and not UDP. The claim has to be supported by publicly available documents	Query - Please clarify what form of supported document will be acceptable by LIC.	Clarification Issued	LIC is looking for threat prevention throughput as published by each OEM. For Checkpoint it is published as "NGTP - Next Generation Threat Prevention" & For Palo Alto it is published as "Threat Prevention". LIC has observed that the data sheets of various models mentions the throughput with desired features in the specifications. LIC is looking for similar reference document from OEM to support the claim.Such documents should be dated prior to the RFP publishing date. Any document other than publicly available documents will be acceptable at the sole discretion of LIC.
64	Tech	2.5	Perimeter DR-NDR	The proposed solution must be able to handle minimum 500 Mbps IPSEC VPN throughput	Need to know parameters on arriving this throughput	These specifications are for DR and NDR . LIC is planning to provide VPN connectivity to remote branches with access to limited users .	No Change

65	Tech	2.6	Perimeter DR-NDR	The proposed solution must support minimum 500 Site to Site IPSEC VPN tunnels. The proposed solution must support minimum 500 Remote / Mobile Access VPN Connections. All licenses needs to be provisioned from day one.	Query - Please clarify if 500 Remote / Mobile access VPN connections are required client - to - site VPN connections	Please be guided by the RFP	
66	Tech	3.1	Perimeter DR-NDR	The proposed solution must support, Port mirroring, Transparent, Layer 2 , Layer 3 mode providing flexibile deployment.	Query - Please clarify if all these / more than one mode required simultaneously.	LIC would prefer all modes simultaneosuly.However its not mandatory	No Change
67	Tech	3.13	Perimeter DR-NDR	The proposed solution must have Virtual Router capabilities that supports all L3 capabilities.The proposed solution must have IPv6 Static Routing Support even for virtual routers.	Need to know the use case and business need of Virtual Routers as there are no virtual firewalls.	Deleted	
68	Tech	3.15	Perimeter DR-NDR	The OEM must provide 24 X 7 X 365 highest level of technical support. The OEM must provide the dedicated login credentials to LIC with highest level permissions to search knowledge base, downloading of the patches, documents and to manage the device. LIC should be able to raise tickets directly to OEMs	Query - Please clarify if LIC is looking for Direct Enterprise Support from OEM	Clarification Issued	In addition to what is stated in the specification LIC wants enterprise and direct OEM support/contract .Its should be the highest level of support which could come under different names for different OEMS.
69	Tech	4.13	Perimeter DR-NDR	The proposed solution must support user-identification over wireless by integrating with Wireless controllers.	Need to know the use case and expectation on integration.	LIC is currently using Wireless infrastructre from Cisco. LIC would like to integrate Cisco Wireless solution with NGFW for user-identification.	No Change
70	Tech	4.13	Perimeter DR-NDR	The proposed solution must support user-identification over wireless by integrating with Wireless controllers.	Query - Please clarify what Wireless infrastructure LIC is using? As firewall will be required to integrate with the same.	LIC is currently using Wireless infrastructre from Cisco. LIC would like to integrate Cisco Wireless solution with NGFW for user-identification.	No Change
71	Tech	4.2	Perimeter DR-NDR	The proposed solution should provide seamless AD Integration with multiple deployment options like Clientless, Captive Portal or Identity Agent on endpoints. The proposed solution must support authentication services for user-identification using all of the following technologies AD, LDAP, 2FA, eDirectory, Radius, Kerberos, Client Certificate from day one. The Solution must include User Directory capabilities to integrate over LDAP.	We would like to know if LIC is using eDirectory and need to know usecase of having user integration with the same.Incase,OEM doesnot support eDirectory integration.	Modified	The proposed solution should provide seamless AD Integration with multiple deployment options like Clientless, Captive Portal or Identity Agent on endpoints. The proposed solution must support authentication services for user-identification using all of the following technologies AD, LDAP, 2FA, Radius, Kerberos, Client Certificate from day one. The Solution must include User Directory capabilities to integrate over LDAP.
72	Tech	4.4	Perimeter DR-NDR	The proposed solution must support Policy Based forwarding based on Zone, Applications , Network, Source / Destination Address, User or User Group	Certain vendors address Zone Based concepts via different ways currently and not necessarily as Zone Based Naming. Zone Based Naming conventions are part of next release	It is acceptable to LIC if bidder is providing necessary support document that this feature will be available in the next release in the near future. Please clearly mention time line, cost & any other relevant details.	No Change
73	Tech	4.6	Perimeter DR-NDR	The proposed solution must be able to handle unknown/unidentified applications e.g. alert, block or allow	Query - Please clarify what does LIC mean by unknown / un-identified applications.	LIC would like to implement positive security model and hence would like to identify all applications traversing in the network currently. It may require to create some custom app signature to identify home made applications. Over and above these application if any traffic is traversing across LIC network, can be classified as Unknown traffic. LIC would like to have complete control of such traffic and should able to Alert, Block or Allow such traffic as per LIC needs.	No Change

74	Tech	4.7	Perimeter DR-NDR	The proposed solution must be able to create custom application signatures and categories based on LIC environment.	Query - Please clarify if LIC want to create custom application for HTTP / HTTPS / TCP based application. In case of HTTPS will LIC allow SSL Decryption?	LIC would like to create custom application signature for home grown applications. It may use HTTP, HTTPS, TCP, UDP etc for communication. NGFW must have capability to create application signature irrrespective of protocols used. It will be preferred if the signature can be creaetd for HTTPS traffic without decryption. LIC would like to keep choice with them to decypt traffic.	No Change
75	Tech	5.1	Perimeter DR-NDR	The proposed solution must provide IPS , Anti Virus, Anti Bot & Spyware Protection features from day one. Integrated IPS must have been tested by NSS LABS & secured recommended rating recently (last 2 years)	Integrated IPS is a part of NGFW and since LIC is considering NGFW solution hence need to consider NSS Report of NGFW. Should consider latest report only as NSS conducts multiple test every year and its not possible to participate in all the testing conducted by NSS.	Modified	The proposed solution must provide IPS, Antivirus, AntiBot & Spyware protection features form day one.Integrated IPS must have been tested NSS labs & secured recommended rating in the last test in which it has particpated .
76	Tech	5.22	Perimeter DR-NDR	The proposed solution must provide flexibilty to detect and prevent Zero Day attacks.	Query - Please clarify is LIC is looking for Zero Day Prevention / APT solution. Typically it requires dynamic & behavioural analyses of unknown files in a control environment (sand boxing). Sand Boxing can be done over cloud - which will require LIC to send data over internet to OEM cloud hosted out side India. OR an on-premises device need to be deployed in addition to NGFW for sanndboxing. Please clarify what exacly is desired.	Clarification Issued	It is clarified that "The proposed model should provide flexibility to integrate with on-premises sand boxing / APT solution to provide prevention against Zero Day Attacks in future"
77	Tech	5.24	Perimeter DR-NDR	Solution must able to provide Data Leakage Prevention - DLP capabailities to stop Credit Card & other important information leaving from LIC network. All DLP related licenses need to be provided from Day one.	DLP Requirement very Generic - it shall be for Mail Traffic	The minimum requirements for DLP have been mentioned in the specification. Bidder is free to propose additional features.	No Change
78	Tech	5.24	Perimeter DR-NDR	Solution must able to provide Data Leakage Prevention - DLP capabailities to stop Credit Card & other important information leaving from LIC network. All DLP related licenses need to be provided from Day one.	Specific Function not clearly defined, Perimeter firewall are PCI Compliant solution, web traffic can be handled for such requirement. Hence we proposed to add Email Protection as well through Dedicated Email Security Solution.	The minimum requirements for DLP have been mentioned in the specification. Bidder is free to propose additional features.	No Change
79	Tech	5.24	Perimeter DR-NDR	Solution must able to provide Data Leakage Prevention - DLP capabailities to stop Credit Card & other important information leaving from LIC network. All DLP related licenses need to be provided from Day one.	Need more info on DLP as why are we asking basic DLP features only and not more advanced like fingerprinting,watermarking, out of box DLP policies, supported file-types etc. DLP solution should focus on advance Data Prevention capabilities and not just Credit Card.	The minimum requirements for DLP have been mentioned in the specification. Bidder is free to propose additional features.	No Change
80	Tech	5.31	Perimeter DR-NDR	Monitor web communication for potential executable code, confirms the presense of executable code and identifies whether the executable code is malicious	Need to know the use case and LIC's expectation from the solution	LIC would like to detect any malicious payload / files traversing during web communication and provide prevention against it.	No Change
81	Tech	5.34	Perimeter DR-NDR	Threat events/protection exclusion rules can be created and view packet data directly from log entries with RAW Packets and if required can be sent to Wireshark for the analysis.	Query - Please clarify if LIC requires data packet capture on Firewall / Management device for security incident such as virus, spyware etc.	LIC desire to capture the raw packets on Firewall for any security event, rule, based on custom filter etc.	No Change
82	Tech	5.36	Perimeter DR-NDR	Customize security profiles for specifc set of Services including IPS etc	Are we setting up Server or Firewall[Typo mistake]	LIC would like to have the flexiblity to create custom security profiles for critical servers	No Change
83	Tech	5.36	Perimeter DR-NDR	Customize security profiles for specifc set of Services including IPS etc	It seems it’s a typo mistake	LIC would like to have the flexiblity to create custom security profiles for critical servers	No Change
84	Tech	5.8	Perimeter DR-NDR	The proposed solution must support different actions in the policy such as deny, drop, reset client, reset server, reset both client and server.	In case of action related to Detect, Prevent and Drop are considered Reset of Client and Server are not required hence not required.	Modified	The proposed solution must support different actions in the policy such as alert/detect,prevent/deny,drop,packet capture

85	Tech	6.3	Perimeter DR-NDR	The proposed solution must support decryption and inspection of SSL traffic in an outbound connection, inbound connection across any port.	Ned to know use case of SSL on any port.	LIC is running many application on non-generic TCP ports such as http is running on 8080 etc. Similalry https is also running on non-generic ports (other than 443). LIC would like to have the ability to detect SSL on such ports & decrypt it if desired.	No Change
86	Tech	6.5	Perimeter DR-NDR	The proposed solution must support on appliance Per policy SSL and SSH decryption for both inbound and outbound traffic.	Why SSH Decryption needed	Modified	The proposed solution must support on appliance Per policy SSL decryption for both inbound and outbound traffic.Proposed solution should support identification and inspection of SSH traffic
87	Tech	6.5	Perimeter DR-NDR	The proposed solution must support on appliance Per policy SSL and SSH decryption for both inbound and outbound traffic.	Specific Function can be best achieved with Dedicated SSH Traffic security solution	Modified	The proposed solution must support on appliance Per policy SSL decryption for both inbound and outbound traffic.Proposed solution should support identification and inspection of SSH traffic
88	Tech	6.5	Perimeter DR-NDR	The proposed solution must support on appliance Per policy SSL and SSH decryption for both inbound and outbound traffic.	Need to know the use case of SSH decryption and impact incase,OEM doesnot support the feature.	Modified	The proposed solution must support on appliance Per policy SSL decryption for both inbound and outbound traffic.Proposed solution should support identification and inspection of SSH traffic
89	Tech	6.6	Perimeter DR-NDR	The SSL decryption throughput should be minimum 10% of the overall throughput as mentioned above .	What is the benchmarking to arrive at 10% of HTTPS Throughput when Industry SSL traffic is gorwing at the rate of more than 18%-20%.	The said performance is minimum requirement of LIC and bidder is free to propose higher throughput.	No Change
90	Tech	6.6	Perimeter DR-NDR	The SSL decryption throughput should be minimum 10% of the overall throughput as mentioned above .	Query - Please clarify if it needs to be minimum 200 Mbps.	Please be guided by the RFP	No Change
91	Tech	8.1	Perimeter DR-NDR	Dedicated management solution must be provided for management, logging and reporting. End to End infrastructure in this regards has to be provided by the vendor. Management and reporting solution is required at DC, DR. They should be in realtime sync	Query - Please clarify if bidder is proposing virtual management platform does it also need to include Server, OS etc.	Please be guided by the RFP	No Change
92	Tech	8.18	Perimeter DR-NDR	The management solution must have automated workflow feature to include management aproval for changes to be applied in firewall cofiguration.	Query - The foresaid feature is only available with one firewall vendor. Request LIC to kindly modify it to be more generic. It can be "The management solution must have third party integration capabilities with broader Eco System partner to achieve multiple functionalities inluding Firewall Chanage Management & Automation. Management solution must provide integration using API."	Deleted	
93	Tech	8.3	Perimeter DR-NDR	Solution should support minimum 6 TB of storage space for logs and reporting.	Query - Please clarify if storage is required with redundancy. Also if 6TB is pre-raid or post raid (usable storage).	Clarification Issued	Solution should support minimum 6 TB of usable storage space for logs and reporting along with RAID-5 redundancy.
94	Tech	3.14.5	Perimeter DR-NDR	Dual (redundant) AC power supply with Indian standard compatible power cords.	Query - Request LIC to allow vendors to propose NGFW with single power supply as well since LIC will be deploying HA Cluster where two firewall can be connected through different power source and failure of one power source will affect one firewall only. This will trigger the HA and traffic will be seamlessly failover to secondary Firewall. LIC will gain following advantage - 1- Rack Space requirement will be lower i.e. instead of 2U it will only require 1U. 2 - Less power utilization. 3 - Less Cable & power point requirement.	Please be guided by the RFP	No Change
95	Tech	3.14.5	Perimeter DR-NDR	Dual (redundant) AC power supply with Indian standard compatible power cords.	Requirement is not clearly defined	Please be guided by the RFP	No Change
96	Tech	3.14.5	Perimeter DR-NDR	Dual (redundant) AC power supply with Indian standard compatible power cords.	Perimeter or Core Firewalls shall not rely on External Dual Power Supply. Using term for integrated will allow positioning of firewall with external dual power supplies. Hence we propose to amend more specifically defined requirement.	Please be guided by the RFP	No Change

97	Tech	1.10	Core DC	The Proposed hardware & product model should be available from OEM at least for 1 year and should not be end of support for next 7 years.	Appliance refresh cycle practice in Industry is 5-7 years and even LIC is doing a refesh after 5 years. OEM should be taking ownership and delivering commitment on the same. This looks like latest applinaces from the OEM should not qualify.	Please be guided by the RFP	No Change
98	Tech	1.11	Core DC	The OEM must provide minimum 3 reference customer of same hardware & product model in India. This should be operational for minimum 12 months preceeding the date of RFP.	All firewall vendors keep upgrading internal hardware (ex-CPU, memory etc.) of their firewall models on regular basis to cater increasing load of industries dynamic infrastructure need due to which they release new models. Generally new models means better compute resources. So we request LIC to relax this clause or at least accept customer references of same model no. with previous series. And anyway vendors are quoting support contract in which they are bound to replace the hardware in case of any fault.	Please be guided by the RFP	No Change
99	Tech	1.2	Core DC	The proposed application security solution must be in the Leader’s or Challengers quadrant in the Gartner "Magic Quadrant for Enterprise Network Firewalls" as per the latest available report.	Contradictory Statement - Application Security is specific function to achieve Secure Application Delivary/accessibility. Asking for Gartner's Quadrant Leader for Enterprise Firewall doesnot make sence	Please be guided by the RFP	No Change
100	Tech	1.2	Core DC	The proposed application security solution must be in the Leader’s or Challengers quadrant in the Gartner "Magic Quadrant for Enterprise Network Firewalls" as per the latest available report.	Achieving the Leader's Level is purely on Business Volume of OEM in respective Segment. Hence we propose as per Suggestion. And also propose to add an option with Gartner's Quadrant or NSSLabs Recommendation with above 96% of rating for Security Value Map in latest report	Please be guided by the RFP	No Change
101	Tech	1.6	Core DC	The appliance hardware should be a multicore CPU architecture with a hardened 64 bit operating system to support higher memory.	LIC should consider Security Effectiveness of NSS NGFW test. Since this tender is for NGFW only NGFW test conducted conduted by NSS in 2016 should be considered and not any other.	Please be guided by the RFP	No Change
102	Tech	1.8	Core DC	The proposed appliance must have at least 8 x 1G Copper Ports from day one. It should be expandable to total 16 x 1G ports and 2 x 10G ports.	**Query** - 1-Please clarify if 16 x 1G & 4 x 10G required from day one. 2- if all ports need to be Data / Production Ports exclusive of management + sync ports. 3- If 16x1G & 4x10G to be achieved simultaneously.	Clarification Issued	The proposed appliance must have at least 8 x 1G Copper Ports from day one. It should be expandable to total 16 x 1G ports and 2 x 10G ports. Management,sync,HA etc ports should be additional
103	Tech	2.1	Core DC	The proposed solution must provide minimum 5 Gbps of throughput (i.e. it should support 5 Gbps of ingress traffic and 5 Gbps of outgress traffic simultaneously) based on multiprotocol performance & real world traffic and not UDP. The claim has to be supported by publicly available documents	Query - Please clarify what form of supported document will be acceptable by LIC.	Clarification Issued	LIC is looking for throughput as published by each the OEMS. LIC has observed that the data sheets of various models data mentions the throughput with desired features in the specifications. LIC is looking for similar reference document from OEM to support the claim.Such documents should be dated prior to the RFP publishing date.Any document other than public reference will be acceptable at the sole discretion of LIC.

104	Tech	2.5	Core DC	Proposed firewall shall support Multiple Security Context/Virtual Firewall/Tenants to be used if need arises	Segmentation will be done on Core Switch[s]	No such query in specifications	
105	Tech	2.5	Core DC	Proposed firewall shall support Multiple Security Context/Virtual Firewall/Tenants to be used if need arises	This Function shall be Optional but not Specific. Since the Segmentation of Network give best result if configured on Core Switch[s]. Firewall can run security processes for Multiple defined segments without configured with Virtual Context/Multiple tenants as well. Hence we propose not to limit only to this function and make it as optional	No such query in specifications	
106	Tech	5.4	Core DC	It shall provide network segmentation features with powerful capabilities that facilitate deploying security for various internal, external, and DMZ subgroups on the network to prevent unauthorized access. There shall be support for detection of reconnaissance attampt such as IP address sweep and port scannig etc.	These are the functionalities of DDOS and are more applicable at the perimeter. Hence we request you to change this clause as "It shall provide network segmentation features with powerful capabilities that facilitate deploying security for various internal, external, and DMZ subgroups on the network to prevent unauthorized access".	Deleted	
107	Tech	3.1	Core DC	The proposed solution must support, Transparent, Layer 2 , Layer 3 mode providing flexibile deployment.	Query - Please clarify if all these / more than one mode required simultaneously.	LIC would prefer all modes simultaneosuly.However its not mandatory	No Change
108	Tech	3.15	Core DC	The OEM must provide 24 X 7 X 365 highest level of technical support. The OEM must provide the dedicated login credentials to LIC with highest level permissions to search knowledge base, downloading of the patches, documents and to manage the device. LIC should be able to raise tickets directly to OEMs.	Query - Please clarify if LIC is looking for Direct Enterprise Support from OEM	Clarification Issued	In addition to what is stated in the specification LIC wants enterprise and direct OEM support/contract .Its should be the highest level of support which could come under different names for different OEMS.
109	Tech	5.2	Core DC	The firewall shall provide robust access control capability and be fast in making access control decisions. Access Control shall be done based on criteria such as source, destination IPs, port number, protocol, traffic type, application, date information (day of week, time of day), etc.	Clause no. 5.2 mentions access control shall be done based on "application" also. Please elaborate the requirement. If LIC wants to create access control policies based on applications which use dynamic ports and protocols like "Microsoft Office 365", "Skype" etc. then Application Control license is required on firewall. Does vendor need to include Application Control license also in proposal?	Clarification Issued	It is clarified that firewall should have the capablities to provide for the performance mentioned in the specifications.
110	Tech	7.3	Core DC	The proposed firewall must support real-time bandwidth statistics of QoS classes.	This functionality should be done at the perimeter. Hence we request you to remove this clause	Please be guided by the RFP	No Change
111	Tech	8.1	Core DC	Dedicated management solution must be provided for management, logging and reporting. End to End infrastructure in this regards has to be provided by the vendor. Management and reporting solution is required at DC, DR. They should be in realtime sync.	Query - Please clarify if bidder is proposing virtual management platform does it also need to include Server, OS etc.	Please be guided by the RFP	No Change
112	Tech	8.3	Core DC	Solution should support minimum 6 TB of storage space for logs and reporting.	Query - Please clarify if storage is required with redundancy. Also if 6TB is pre-raid or post raid (usable storage).	Clarification Issued	Solution should support minimum 6 TB of usable storage space for logs and reporting along with RAID-5 redundancy.
113	Tech	8.4	Core DC	Solution must provide log analysis and policy management, any tool which is required for providing the same must be included in offering.	Log will be forwarded to the SIEM used by LIC. Hence we request you to remove log analysis from this clause	Please be guided by the RFP	No Change

114		7.1.2	Core DC	by user/user group as defined by AD	Advance QoS is to be done at the perimeter. Hence we request you to remove this clause	Modified	QoS by user/user group as defined by AD/IP Address
115	Tech	3.14.5	Core DC	Integrated Dual (redundant) AC power supply with Indian standard compatible power cords.	Generally with all firewall vendors integrated(inbuilt) redundant power supply starts with large data center grade appliances which is not the case as per technical specifications mentioned in this RFP. So to comply to this clause all firewall vendors have to propose higher-end appliance which will hike to cost unnecessarily. So we request LIC to accept external redundant power supply also for redundancy purpose and change clause to "Integrated or external dual (redundant) AC power supply with Indian standard compatible power cords"	Please be guided by the RFP	No Change
116	Tech	3.14.5	Core DC	Integrated Dual (redundant) AC power supply with Indian standard compatible power cords.	Requirement is not clearly defined	Please be guided by the RFP	No Change
117	Tech	3.14.5	Core DC	Integrated Dual (redundant) AC power supply with Indian standard compatible power cords.	Perimeter or Core Firewalls shall not rely on External Dual Power Supply. Using term for integrated will allow positioning of firewall with external dual power supplies. Hence we propose to amend more specifically defined requirement.	Clarification Issued	Only integrated (internal) dual redundant power supply required with Indian standard compatible power cords .
118	Tech	1.11	Core DR-NDR	The OEM must provide minimum 3 reference customer of same hardware & product model in India. This should be operational for minimum 12 months preceeding the date of RFP.	All firewall vendors keep upgrading internal hardware (ex-CPU, memory etc.) of their firewall models on regular basis to cater increasing load of industries dynamic infrastructure need due to which they release new models. Generally new models means better compute resources. So we request LIC to relax this clause or at least accept customer references of same model no. with previous series. And anyway vendors are quoting support contract in which they are bound to replace the hardware in case of any fault.	Please be guided by the RFP	No Change
119	Tech	1.11	Core DR-NDR	The OEM must provide minimum 3 reference customer of same hardware & product model in India. This should be operational for minimum 12 months preceeding the date of RFP.	Appliance refresh cycle practice in Industry is 5-7 years and even LIC is doing a refesh after 5 years. OEM should be taking ownership and delivering commitment on the same. This looks like latest applinaces from the OEM should not qualify.	Please be guided by the RFP	
120	Tech	1.8	Core DR-NDR	The proposed appliance must have at least 8 x 1G Copper Ports from day one. It should be expandable to total 16 x 1G ports.	Can we request you to modify this clause as "The proposed appliance must have 8 x 1G copper ports from day one. It should be expandable to total 14 x 1G ports".	Modified	The proposed appliance must have at least 8 x 1G Copper Ports from day one. It should be expandable to total 14 x 1G ports .Management,sync,HA etc ports should be additional

121	Tech	2.1	Core DR-NDR	The proposed solution must provide minimum 2 Gbps of throughput (i.e. it should support 2 Gbps of ingress traffic and 2 Gbps of outgress traffic simultaneously) based on multiprotocol performance & real world traffic and not UDP. The claim has to be supported by publicly available documents	Query - Please clarify what form of supported document will be acceptable by LIC.	Clarification Issued	LIC is looking for throughput as published by each the OEMS. LIC has observed that the data sheets of various models data mentions the throughput with desired features in the specifications. LIC is looking for similar reference document from OEM to support the claim.Such documents should be dated prior to the RFP publishing date.Any document other than public reference will be acceptable at the sole discretion of LIC.
122	Tech	2.5	Core DR-NDR	Proposed firewall shall support Multiple Security Context/Virtual Firewall/Tenants to be used if need arises	Segmentation will be done on Core Switch[s]	Please be guided by RFP	No Change
123	Tech	2.5	Core DR-NDR	Proposed firewall shall support Multiple Security Context/Virtual Firewall/Tenants to be used if need arises	This Function shall be Optional but not Specific. Since the Segmentation of Network give best result if configured on Core Switch[s]. Firewall can run security processes for Multiple defined segments without configured with Virtual Context/Multiple tenants as well. Hence we propose not to limit only to this function and make it as optional	Please be guided by RFP	No Change
124	Tech	2.6	Core DR-NDR	It shall provide network segmentation features with powerful capabilities that facilitate deploying security for various internal, external, and DMZ subgroups on the network to prevent unauthorized access. There shall be support for detection of reconnaissance attampt such as IP address sweep and port scannig etc.	These are the functionalities of DDOS and are more applicable at the perimeter. Hence we request you to change this clause as "It shall provide network segmentation features with powerful capabilities that facilitate deploying security for various internal, external, and DMZ subgroups on the network to prevent unauthorized access".	Deleted	
125	Tech	3.1	Core DR-NDR	The proposed solution must support, Port mirroring, Transparent, Layer 2 , Layer 3 mode providing flexibile deployment.	Query - Please clarify if all these / more than one mode required simultaneously.	LIC would prefer all modes simultaneosuly.However its not mandatory	No Change
126	Tech	3.15	Core DR-NDR	The OEM must provide 24 X 7 X 365 highest level of technical support. The OEM must provide the dedicated login credentials to LIC with highest level permissions to search knowledge base, downloading of the patches, documents and to manage the device. LIC should be able to raise tickets directly to OEMs.	Query - Please clarify if LIC is looking for Direct Enterprise Support from OEM	Clarification Issued	In addition to what is stated in the specification LIC wants enterprise and direct OEM support/contract .Its should be the highest level of support which could come under different names for different OEMS.
127	Tech	5.2	Core DR-NDR	The firewall shall provide robust access control capability and be fast in making access control decisions. Access Control shall be done based on criteria such as source, destination IPs, port number, protocol, traffic type, application, date information (day of week, time of day), etc.	Clause no. 5.2 mentions access control shall be done based on "application" also. Please elaborate the requirement. If LIC wants to create access control policies based on applications which use dynamic ports and protocols like "Microsoft Office 365", "Skype" etc. then Application Control license is required on firewall. Does vendor need to include Application Control license also in proposal?	Clarification Issued	It is clarified that firewall should have the capablities to provide for the performance mentioned in the specifications.
128	Tech	7.3	Core DR-NDR	The proposed firewall must support real-time bandwidth statistics of QoS classes.	This functionality should be done at the perimeter. Hence we request you to remove this clause	Please be guided by the RFP	No Change

129	Tech	8.1	Core DR-NDR	Dedicated management solution must be provided for management, logging and reporting. End to End infrastructure in this regards has to be provided by the vendor. Management and reporting solution is required at DC, DR. They should be in realtime sync.	Query - Please clarify if bidder is proposing virtual management platform does it also need to include Server, OS etc.	Please be guided by the RFP	No Change
130	Tech	8.16	Core DR-NDR	The management solution must have automated workflow feature to include management aproval for changes to be applied in firewall cofiguration.	Query - The foresaid feature is only available with one firewall vendor. Request LIC to kindly modify it to be more generic. It can be "The management solution must have third party integration capabilities with broader Eco System partner to achieve multiple functionalities inluding Firewall Chanage Management & Automation. Management solution must provide integration using API."	Deleted	
131	Tech	8.3	Core DR-NDR	Solution should support minimum 6 TB of storage space for logs and reporting.	Query - Please clarify if storage is required with redundancy. Also if 6TB is pre-raid or post raid (usable storage).	Clarification Issued	Solution should support minimum 6 TB of usable storage space for logs and reporting along with RAID-5 redundancy.
132	Tech	8.4	Core DR-NDR	Solution must provide log analysis and policy management, any tool which is required for providing the same must be included in offering.	Log will be forwarded to the SIEM used by LIC. Hence we request you to remove log analysis from this clause	Please be guided by RFP	No Change
133	Tech	7.1.2	Core DR-NDR	by user/user group as defined by AD	Advance QoS is to be done at the perimeter. Hence we request you to remove this clause	Modified	QoS by user/user group as defined by AD/IP Address
134	Tech	3.14.5	Core DR-NDR	Integrated Dual (redundant) AC power supply with Indian standard compatible power cords.	Generally with all firewall vendors integrated(inbuilt) redundant power supply starts with large data center grade appliances which is not the case as per technical specifications mentioned in this RFP. So to comply to this clause all firewall vendors have to propose higher-end appliance which will hike to cost unnecessarily. So we request LIC to accept external redundant power supply also for redundancy purpose and change clause to "Integrated or external dual (redundant) AC power supply with Indian standard compatible power cords"	Please be guided by the RFP	No Change
135	Tech	1.2	Core DR-NDR	The proposed application security solution must be in the Leader’s or Challengers quadrant in the Gartner "Magic Quadrant for Enterprise Network Firewalls" as per the latest available report.	Contradictory Statement - Application Security is specific function to achieve Secure Application Delivary/accessibility. Asking for Gartner's Quadrant Leader for Enterprise Firewall doesnot make sence	Please be guided by RFP	No Change
136	Tech	1.2	Core DR-NDR	The proposed application security solution must be in the Leader’s or Challengers quadrant in the Gartner "Magic Quadrant for Enterprise Network Firewalls" as per the latest available report.	Achieving the Leader's Level is purely on Business Volume of OEM in respective Segment. Hence we propose as per Suggestion. And also propose to add an option with Gartner's Quadrant or NSSLabs Recommendation with above 96% of rating for Security Value Map in latest report	Please be guided by RFP	No Change