Response to the Pre-Bid Queries , Technical Specifications , to the RFP Procurement of Network Gateway Security Products, Implementation & Management. (Next Generation Firewall Solution, Sandbox Solution, DNS Security etc.) Ref: LIC-CO/IT-BPR/FW/RFP/2022-23/01 Dated: 21/10/2022				
Sr. No.	**RFP Document Reference(s) (Section & Page Number)**	**RFP Clause**	**Pre-bid Queries**	**Response**
1	General Requirements (1.3)	For high performance with low latency (maximum 100 Microseconds as per NSS Lab report within last two years for all packet size) the proposed solution must provide all application level inspection. Firewall & Integrated IPSEC VPN Applications should be ICSA Labs certified for ICSA 4.0 & FIPS 140-2 certified. In case NSS Lab reports are not published in the last two years prior to the date of this RFP, the OEM should provide the undertaking on its letterhead signed by a signatory authorised by the board certifying the latency.	We would like to know if the NSS Lab report results for 2019 will work for this point? OR Latency details are required on Letterhead.	Please refer to the revised technical specifications
2	General Requirements (1.10)	Firewall Appliance should have a feature of holding multiple OS images to support resilience & easy rollbacks during the version upgrades	1. Check Point has a different workflow here, the solution takes a snapshot (backup of configuration along with the OS) before version upgrades to have it auto-rollback in case of any issues identified while upgrading. 2. The same Snapshot can be stored externally on another storage 3. The solution has a feature named pre-upgrade verifier which verifies the problem / compatibility of the hotfixes / OS on the current platform and showcases the result to have a seamless & successful upgrade. Requesting LIC team to kindly acknowledge and accept this approach as compliant.	Please refer to the revised technical specifications
3	Performance (2.1)	Cluster based solutios will not be acceptable.	Check Point supports HyperScale solution i.e. Quantum Maestro which is a highly scalable solution. Request LIC to consider the solution OR else remove the Cluster clause.	Please be guided by the RFP
4	Firewall Security Policy (4.1)	The proposed solution must support network traffic classification which identifies applications across all ports irrespective of port/protocol/evasive tactic from day one. The proposed solution must have application and application function identification and decoding technology from day one.	This has parts of patented solution from an OEM, requesting LIC team to remove this point. This enables us to quote.	Please refer to the revised technical specifications
5	Threat Prevention Features (5.1)	The proposed solution must provide IPS, IDS, APT, Antivirus, AntiBot & Spyware protection features from day one. Integrated IPS & IDS must have been tested NSS labs & secured recommended rating in the last test in which it has participated in the last two years from the date of this RFP. In case NSS Lab reports are not published in the last two years prior to the date of this RFP, the OEM should provide the undertaking on its letterhead signed by a signatory authorized by the board certifying the recommended ratings.	We would like to know if the NSS Lab report results for 2019 will work for this point?	Please refer to the revised technical specifications
6	Threat Prevention Features (5.3)	The proposed solution shall perform stream-based Anti-Virus & Anti-Spyware and not store-and-forward traffic inspection	We recommend LIC team to accept both the options as eventually it's the affected file which is getting blocked considering no additional latency or performance is been added in the user experience.	Please refer to the revised technical specifications
7	Threat Prevention Features (5.37.1)	The proposed threat prevention solution should provide prevention against DoS, DDoS attacks for all protocols including TCP and UDP	We request LIC team to minimize the points and remove these parameters as they are use cases of dedicated DDoS solution. Replicating it again on firewall is not a general practice to be	Clause Deleted
8	Threat Prevention Features (5.37.2)	The DoS, DDoS prevention solution should offer syn cookie and threshold base mechanism to identify attacker / DoS, DDoS attacks and block them automatically		Please be guided by the RFP
9	Threat Prevention Features (5.37.3)	It should be able to restrict web infrastructure (HTTP/HTTPS etc.) request from same source and destination		Please be guided by the RFP
10	Threat Prevention Features (5.37.7)	Should have prevention against Script DDoS tool that utilizes high bandwidth webservers to generate malicious DDoS traffic.		Please be guided by the RFP
11	Advanced Persistent Threat Features (6.6)	The solution should incorporate an on-premises sandbox solution deployed at each location with high availability across all sites.	General asked deployments of Sandboxing are cloud service, distributed (passive mode) and inline mode. Sandboxing solutions are not deployed in HA as in case of failures or unreachability the traffic is bypassed from the sandboxing devices providing no impact on the production traffic until the RMA is received. Hence, requesting LIC team to remove this point or amend accordingly.	Please refer to the revised technical specifications

12	Advanced Persistent Threat Features (6.15)	The sandbox appliance should have 16TB RAID storage with capability for future expansion	Check Point solution is designed in a way where the logs are centrally stored on the management server and not on the Threat Emulation device. This is the right use of having a distributed model of working and consolidation to then correlate between events and provide the right indexing. We request LIC team to remove this point.	Please refer to the revised technical specifications
13	SSL Decryption (8.6)	The SSL decryption throughput i.e. decryption and security encryption where IP is AV, Anti-Spyware, APT, ATP, etc should be minimum 50% of the overall throughput above	The sizing will completely change considering 50% of SSL traffic (7.5 Gbps) on the asked throughput. Request LIC team to remove this point OR amend it to the below: The SSL decryption throughput i.e. decryption and security encryption where IP is AV, Anti-Spyware, APT, ATP, etc should be minimum 20% of the overall throughput above.	Please be guided by the RFP
14	Management & Reporting (9.3)	Solution should support minimum 10TB of usable storage space for logs and reporting along with RAID-6 redundancy	We will recommend storing the logs on external device instead on the management server to increase it capabilities OR instead go ahead with a software based option as it is the recommended industry practice to tweak the hardware parameters as per LIC's requirement and is very flexible. Requesting LIC team to amend it to below: The management server can be quoted as a software management so that LIC team has the control on tweaking the specifications as and when required.	Please refer to the revised technical specifications
15	Management & Reporting (9.4)	Solution must provide log analysis and policy management, any tool which is required for providing the same must be included in offering	Log analysis is integrated in the centralized console but for policy management we recommend using dedicated policy analyzer tools available in the market which integrates with popular vendors. Requesting LIC team to amend this point only towards log analysis.	Please be guided by the RFP
16	Management & Reporting (9.19)	Management solution should also have the following operational capabilities: i. Unused Rules Calculation for specific time period based on Firewall Traffic Logs. Ii. Analysis on Covered/Shadow/Hidden Rules iii. Analysis on Rules Consolidation (Merging of similar kind of rules) iv. Analysis on Redundant Rules v. Tightening of Overly Permissive Rules (Any-Any) vi. Analysis on Unattached/Unused Objects to simplify objects management vii. Analysis on Rule-Reordering to improve the performance of the Firewall viii. Analysis on Disabled/Expired Rules for enhanced visibility on Firewall Rules sets	There are dedicated tools available which has these requirements as a part of their use cases and many additional features over it. We would request LIC team to remove this point and have this covered under dedicated tools.	Please be guided by the RFP
17	General Requirements - 1.8	The proposed solution must have minimum 450 GB SSD for storing logs etc. The logs should not be stored on the Firewall.	If the logs should not be stored on the firewall, the firewall would not require large storage. Internal Storage will only be required storing OS file. Request to amend the clause as "The proposed solution must have minimum 24 GB Flash/Internal Storage for storing OS files etc. The logs should not be stored on the Firewall."	Please refer to the revised technical specifications
18	General Requirements - 1.12	The OEM must provide minimum 3 reference customer of same hardware & product model in India.	Considering that the Firewall has to be available with 6 years of support, we would be proposing the latest generation of firewall. Hence we request you to consider the clause as below. "The OEM must provide minimum 3 reference customer of same / similar / higher hardware model in India."	Please be guided by the RFP
19	Performance - 2.1	The proposed solution must provide minimum 15Gbps of throughput (i.e. it should support 15 Gbps of ingress traffic and 15 Gbps of outgress traffic simultaneously) with all security features enabled including Application Control + IPS + Anti Spyware + Anti Bot + Antivirus + DDoS + APT along with all signature turned ON. The performance must be based on HTTP traffic with a transaction size of 64K. The claim has to be supported by publicly available documents published prior to the date of the RFP. The performance requirement is for a single hardware appliance and should not be for a cluster. Cluster based solutions will not be acceptable.	The clause mentions throughput requirement of 15Gbps with ingress throughput of 15Gbps and outgress throughput of 15Gbps simultaneously. The firewall is sized based on the total throughput of the appliance. Irrespective of the direction, traffic will hit and be processed by the CPU of the firewall. Request you to confirm if the throughput should be considered at 30Gbps (aggregation of ingress + outgress traffic).	Please refer to the revised technical specifications

20	Performance - 2.1	The proposed solution must provide minimum 15Gbps of throughput (i.e. it should support 15 Gbps of ingress traffic and 15 Gbps of outgress traffic simultaneously) with all security features enabled including Application Control + IPS + Anti Spyware + Anti Bot + Antivirus + DDoS + APT along with all signature turned ON. The performance must be based on HTTP traffic with a transaction size of 64K. The claim has to be supported by publicly available documents published prior to the date of the RFP. The performance requirement is for a single hardware appliance and should not be for a cluster. Cluster based solutions will not be acceptable.	Public document contains throughput based on enterprise mix of traffic and not HTTP 64K with all the features enabled. We can provide the undertaking on for the throughput. Request to change the clause as "The proposed solution must provide minimum 15 Gbps of throughput (i.e. it should support 15 Gbps of ingress traffic and 15 Gbps of outgress traffic simultaneously) with all threat prevention features turned on. The performance must be based on HTTP traffic with a packet size of 64K. The claim has to be supported by publicly available documents published prior to the date of this RFP or OEM undertaking on Letterhead. The performance requirement is for a single hardware appliance and should not be for a cluster. Cluster based solutions will not be acceptable."	Please be guided by the RFP
21	Performance - 2.6	The proposed solution must support minimum 4000 Site to Site IPSEC VPN tunnels. The proposed solution must support minimum 10000 Remote / Mobile Access VPN Connections. This should include web based SSL VPN, Client based VPN Solution, VPN access through Android, iPhone, MacOS, Linux, Chrome OS. The VPN solution should include capability to perform posture check for system, compliance with such parameters as antivirus health, OS version, domain membership etc. and should restrict access to internal resources based on the compliance status of th system. The VPN solutions should provide access only to the intended applications and should not provide access to entire internal network of LIC to the VPN users. All licenses needs to be provisioned from day one.	Request you to confirm if we should propose licenses for 10,000 users from Day-1.	Please refer to the revised technical specifications
22	Operation Mode - 3.1	The proposed solution must support, Port mirroring, Bridge Mode, Transparent, Layer 2 , Layer 3 mode providing flexibile deployment.	Firewall is either deployed in Bridge (Transparent/ Layer2) mode or NAT mode (Layer3). Port mirroring is used on a network switch to send a copy of network packets seen on one switch port (or an entire VLAN) to a network monitoring connection on another switch port. This is not a firewall feature hence request you to rephrase the point as "The proposed solution must support Bridge Mode, Transparent, Layer 2 , Layer 3 mode providing flexible deployment. "	Please be guided by the RFP
23	Operation Mode - 3.14.6	Dual (redundant) hot swappable fans	The proposed firewall will have in-built redundant FANs to ensure that the internal components are provided sufficient cooling and resiliency to failure. It does not give any additional benefit from a hardware standpoint. Request you to modify the clause as " The Firewall must support redundant FAN."	Please be guided by the RFP
24	Firewall Security Policy - 4.13	The proposed solution must support user-identification over wireless by integrating with Wireless controllers.	Request you to provide more clarity on the integration required between WLC and Firewall?	Please be guided by the RFP
25	Threat Prevention Features - 5.37.2	The DoS, DDoS prevention solution should offer syn cookie and threshold base machanism to identify attacker / DoS, DDoS attacks and block them automatically	While Firewall can provide DOS/DDOS functionality it can never provide granular controls as a dedicated DOS/DDOS appliance. Request you to remove this point as this feature is part of dedicated DDOS solution.	Clause Deleted
26	Threat Prevention Features - 5.37.4	Should have an understanding of DDOS Tool Kit including SYN Flood, UDP Flood, DNS Query flood and GET floods	While Firewall can provide DOS/DDOS functionality it can never provide granular controls as a dedicated DOS/DDOS appliance. Request you to remove DNS query flood and GET floods as this feature is part of DDOS appliance and rephrase the clause as "Should have an understanding of DDOS Tool Kit including SYN Flood, UDP Flood"	Please be guided by the RFP
27	Threat Prevention Features - 5.37.5	Should have protection against exploitation of DOS vulnerability in Microsoft IE, Microsoft IIS, Apache, Oracle etc.	Microsoft has ended support for IE hence request you to remove this point and rephrase the clause as "Should have protection against exploitation of DOS vulnerability in Microsoft IIS, Apache, Oracle etc."	Please be guided by the RFP
28	Threat Prevention Features - 5.37.7	Should have prevention against Script DDoS tool that utilizes high bandwidth webservers to generate malicious DDoS traffic.	While Firewall can provide DOS/DDOS functionality it can never provide granular controls as a dedicated DOS/DDOS appliance. Request you to remove this point as this feature is part of dedicated DDOS solution.	Please be guided by the RFP
29	Advanced Persistent Threat Features - 6.12	The sandbox solution should perform minimum 60 simultaneous file analysis in the sandbox environment.	Scanning of 12,000 files per day averages to 1000 files per hour and approximately 17 files / minute. Considering the average time for completting the scan for single file is 1-3 minutes, 20 VM environments are required simultaneously. Request you to amend the clause as "The sandbox solution should perform minimum 20 simultaneous file analysis in the sandbox environment."	Please refer to the revised technical specifications

30	Advanced Persistent Threat Features - 6.11	The sandbox solution should support analysis of EXE, DLL, MS Office files such as Docx, XLSX; PDF; Flash; Java applets (JAR and CLASS); analysis of links within email messages, compressed (ZIP), script files such as .bat, .vbs, .js, .ps1, .sh in a sandbox environment.	Remove CLASS and .sh file from the clause	Please be guided by the RFP
31	Advanced Persistent Threat Features - 6.15	The sandbox appliance should have 16TB RAID storage with capability for future expansion.	Every VM environment requires bare minimum resource to bring up the OS environment. OS like windows / linux requires 32GB space for 32/64 bit instance. With this calculation 32GB X 60 = 1.92 TB of Space is required. Request you to rephrase the clause as "The sandbox appliance should have 2TB storage with capability for future expansion."	Please refer to the revised technical specifications
32	Advanced Persistent Threat Features - 6.6	The solution should have 10000+ CVE Signatures to protect LIC environment from known exploit attacks.	It is important for the solution to have effective security instead of relying on the number of CVE signatures. Request to rephrase the clause as following "Security effectiveness should be certified by NSS and should be more than 98.5%. In case NSS Lab reports are not published in the last two years prior to the date of this RFP, the OEM should have AAA rating published by Cyber rating report in 2021 ."	Please be guided by the RFP
33	Management & Reporting - 9.3.1	The solution has to provide for taking backups in encrypted in SHA-256 format.	Every vendor uses different encryption methods to encrypt the backup files. We support AES-128. Request you to rephrase the clause as "The solution has to provide for taking backups in encrypted in SHA-256 / AES/128 format."	Please refer to the revised technical specifications
34	Management & Reporting - 9.5	The solution must be able to segment the rule based sub policy structures in which only the relevant traffic is being forwarded to relevant policy.	Request you to provide more clarity on the requirement and the use case.	Please be guided by the RFP
35	Management & Reporting - 9.9	The Firewall logs must contain information about the firewall policy rule that triggered the log. Should support google like search of logs within seconds	Providing Google like search is specific to a vendor hence request you to rephrase the clause as "The Firewall logs must contain information about the firewall policy rule that triggered the log."	Please be guided by the RFP
36	Management & Reporting - 9.19	Management solution should also have the following operational capabilities: i. Unused Rules Calculation for specific time period based on Firewall Traffic Logs. ii. Analysis on Covered/Shadow/Hidden Rules iii. Analysis on Rules Consolidation (Merging of similar kind of rules) iv. Analysis on Redundant Rules v. Tightening of Overly Permissive Rules (Any-Any) vi. Analysis on Unattached/Unused Objects to simplify objects management vii. Analysis on Rule-Reordering to improve the performance of the Firewall viii. Analysis on Disabled/Expired Rules for enhanced visibility on the Firewall Rules sets	Features like Rule consolidation, overly permissive rule and rule reordering are supported by single OEM within the solution. Request you to remove these points from the requirement.	Please be guided by the RFP
37	Management & Reporting - 9.3	Solution must support adding exceptions to IPS enforcement from the log record	As log access is available with different levels of administrator, this feature can lead to security concerns if IPS exceptions are added which can lead to bypassing of genuine attacks. Request you to remove this clause.	Clause Deleted
38	Event Corelation and Best Practices - 10.4	Vendor must have an option to Deliver real-time assessment of compliance with major regulations (PCI-DSS,HiPPA,SOX etc.)	PCI reports are more relevant to the Financial industry while HIPPA is required for Health care organizations. Request you to rephrase the point as "Vendor must have an option to Deliver real-time assessment of compliance with major regulations (PCI-DSS etc)"	Please be guided by the RFP
39	API Automation - 11.3	The solution should support Management API for IoC Blocking	Request you to provide more clarity on the requirement and the use case.	Please be guided by the RFP
40	API Automation - 11.4	The solution should support Add, delete, and view indicators through the management API	Request you to provide more clarity on the requirement and the use case.	Please be guided by the RFP
41	Advanced Persistent Threat Features 6.12	The sandbox solution should perform minimum 60 simultaneous file analysis in the sandbox environment	Sandboxing solutions are sized based on number of Unique files per hour OR Throughput OR Virtual Machines expected in the sandboxing for emulation. The stated parameter won't be a right fit for the requirement. Hence requesting LIC team to amend it to below: The sandboxing solution should provide 2.5 Gbps of throughput with minimum of 25 virtual machines.	Please refer to the revised technical specifications