Corrigendum 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**	
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.	Kindly refer to the revised technical specifications
2	General Requirements (1.9)	The proposed appliance must have at least 12x1G Copper Ports from day one. The appliance should have 8 x 10G SFP+ ports, 2 x 25G QSFP 28 Ports and 2 x 40G QSFP ports. Management, sync, HA etc ports should be additional. All the modules and transceivers should be provided from day one.	This hardware specifications are pertaining to a specific OEM. Request relaxation of this clause as the number of ports asked are substantially high as compared to the expected throughput of 5Gbps. Request LIC team to ammend the interfaces as the following: 1. 12x1G Copper 2. 4x10G SFP+ (Slot1) 3. 4x10G SFP+ (Slot2) Additional 2x40G (Per slot) interfaces can be accomodated by replacing the existing network interfaces cards.	Please refer to the revised technical specifications .
3	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 .
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 followed. Preventing against vulnerabilities which can be abused to initiate DDoS is a valid expectation from Firewall.	Clause Deleted
8	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 .
9	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 .
10	Management & Reporting (10.3)	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 .

11	General Requirements - 1.8	The proposed solution must have minimum 240 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 .
12	Performance - 2.1	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 + 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 shouuld not be for a cluster. Cluster based solutions will not be acceptable.	The clause mentions throughput requirement of 5Gbps, with ingress throughput of 5Gbps and outgress throughput of 5Gbps 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 10Gbps (aggregation of ingress + outgress traffic).	Please refer to the revised technical specifications .
13	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 refer to the revised technical specifications .
14	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 32/30 bit instance. With this calculation 32GB X 60 = 960 GB of Space is required. Request you to rephrase the clause as "The sandbox appliance should have 1TB storage with capability for future expansion."	Please refer to the revised technical specifications .
15	Management & Reporting - 10.3.1	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 .
16	Management & Reporting - 10.30	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
17	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 .
18	1.9	The proposed appliance must have at least 12 x 1G Copper Ports from day one. The appliance should have 8 x 10G SFP+ ports, 2 x 25G QSFP 28 Ports and 2 x 40G QSFP ports. Management,sync,HA etc ports should be additional. All the modules and transceivers should be provided from day one.	Request LIC to modify this to: "The proposed appliance must have at least 12 x 1G Copper Ports from day one. The appliance should have 8 x 10G SFP+ ports, 2 x 25G QSFP 28 Ports. Management,sync,HA etc ports should be additional. All the modules and transceivers should be provided from day one."	Please refer to the revised technical specifications .
19	3.14.7	Dual (redundant) SSD	Request LIC to modify this to: Appliance should have SSD	Please refer to the revised technical specifications .
20	2.3	The proposed solution must be able to handle minimum 15,00,000 concurrent sessions with all the Layer 7/ Application Layer Security features /APT turned ON.	Request LIC to modify this in order to bring it in line with the Core IDC Yog firewall: The proposed solution must be able to handle minimum 12,00,000 concurrent sessions with all the Layer 7/ Application Layer Security features /APT turned ON.	Please refer to the revised technical specifications .
21	Operation Mode - 3.14.6	Dual (redundant) hot swappable fans	Request LIC to modify this to: Dual (redundant) fans	Please refer to the revised technical specifications .
22	1.9	The proposed appliance must have at least 12 x 1G Copper Ports from day one. The appliance should have 8 x 10G SFP+ ports, 2 x 25G QSFP 28 Ports and 2 x 40G QSFP ports. Management,sync,HA etc ports should be additional. All the modules and transceivers should be provided from day one.	Request LIC to modify this to: "The proposed appliance must have at least 12 x 1G Copper Ports from day one. The appliance should have 8 x 10G SFP+ ports, 2 x 25G QSFP 28 Ports. Management,sync,HA etc ports should be additional. All the modules and transceivers should be provided from day one."	Please refer to the revised technical specifications .
23	3.14.6	Dual (redundant) hot swappable fans	Request LIC to modify this to: Dual (redundant) fans	Please refer to the revised technical specifications .
24	3.14.7	Dual (redundant) SSD	Request LIC to modify this to: Appliance should have SSD	Please refer to the revised technical specifications .
25	2.3	The proposed solution must be able to handle minimum 15,00,000 concurrent sessions with all the Layer 7/ Application Layer Security features /APT turned ON.	Request LIC to modify this in order to bring it in line with the Core IDC Yog firewall: The proposed solution must be able to handle minimum 12,00,000 concurrent sessions with all the Layer 7/ Application Layer Security features /APT turned ON.	Please refer to the revised technical specifications .