Response to Queries - Bid Reference No: GEM/2020/B/586453 dated 06.03.2020 and ATC document dated 06.03.2020 (Supply, installation and commissioning of NGFW equipment)							
SN	**ATC Clause No.**	**Page No**	**Tender / ATC Clause detail**	**Amendment Sought / Suggestion**	**Justification**	**Firm's Name**	**PSeGS response**
1	15.9	3	New Session/Connection per second: 450K or higher	New Session/Connection per second 450K and should be scalable upto 550K using same solution	There should be scalablitiy for better ROI	Checkpoint	As per ATC document
2	15.21	3	Storage Capacity (GB): 4,000 or higher	Storage Capacity (GB) 2000	2 TB is sufficient as per requirement .	Checkpoint	Refer Corrigendum
3	15.29	3	Interface Expansion slots supported: 2	Interface Expansion slots supported 5	There should be atleast 5 expansion slot seeing requirement	Checkpoint	Refer Corrigendum
4	16 (a)	4	NGFW throughput (real world / enterprise mix): 30 Gbps	Solution Should ensure Minimum 22 GbpS Threat Protection Throughput (NGFW + URL Filtering + IPS + Antivirus + AntiBot/Anti Spyware/Anti Malware + Zero Day) at any point of time, with logging enabled and tested with Enterprise Mix/Application Mix/ Production traffic/Real World Traffic	In Gem Specs all features are asked like bot protection, AV APT etc but in general specs NGFW is mentioned, which should be threat protection throughput	Checkpoint	As per ATC document

5	16 (f)	4	Sandbox: There should be separate appliance for zero day / sandbox / ATP with minimum 4x 1 GE SFP and 4 x RJ 45, 2x2 TB storage on-appliance in RAID 1, minimum 20 VMs support, VM sandboxing throughput of minimum 1,000 file per hour and sniffer throughput of 2 Gbps and should have all Win / Linux OS (which are not out of support) and MS office licenses from day 1. In case of appliance failure, there should be provision of HA appliance for redundancy with equivalent sandboxing throughput of 1,000 files per hour.	Sandbox: There should be separate appliance for zero day / sandbox / ATP with minimum 4 x RJ 45, 2x2 TB storage on-appliance in RAID 1, minimum 20 VMs support, VM sandboxing throughput of minimum 1,000 file per hour and sniffer throughput of 2 Gbps and should have all Win / Linux OS (which are not out of support) and MS office licenses from day 1. In case of appliance failure, there should be provision of HA appliance for redundancy with equivalent sandboxing throughput of 1,000 files per hour and APT appliance should be deployed in inline mode.	4 x RJ 45 port is enough for sandboxing appliance so please remove additional port. APT should be in inline mode then only zero day attack will be prevented	Checkpoint	Refer Corrigendum
6	16 (s)	5	Ability to detect, log and take action against network traffic based on over 4,000+ application signatures	Ability to detect, log and take action against network traffic based on over 7,000 (excluding custom signature) application signatures	4000 is very less signature for applications. Please make it to 7000+	Checkpoint	As per ATC document
7	NA	NA	New Point	The Proposed Firewall Vendor should be in the Leaders' Quadrant of the latest Gartner Magic Quadrant for Enterprise Firewalls since past 3 years and there should be no vulnerability in firewall OS since past 3 years	As firewall is mission critical device there should be no vulnerability in firewall OS. It becomes very easy for hackers to bypass when there is any vulnerability and penitrate ino network. **Reference:** https://www.zdnet.com/article/iranian-hackers-have-been-hacking-vpn-servers-to-plant-backdoors-in-companies-around-the-world/	Checkpoint	As per GeM bid / ATC document

8	NA	NA	New Point	OEM should have more then 95% Security effectivness in all NSS Breach Prevention Test Report i.e (2017&2019)	NSS test firewall with real malwares and publish report .	Checkpoint	As per GeM bid / ATC document
9	15.8	3	Concurrent Session/Concurrent Connection : 30M or higher	request to change" Concurrent Session/Concurrent Connection : 25M"	30M Concurrent session are on very higher side for asked throughput so request kindly consider our query to bring all OEMs on similar hardware configuration.	Cisco	As per ATC document
10	15.9	3	New session/Connection per second: 450K or higher	request to change" New session/Connection per second: 500K"	500K New session/Connection per second are on very higher side for asked throughput so request kindly consider our query to bring all OEMs on similar hardware configuration.	Cisco	As per ATC document
11	15.13	3	Number of QSFP+ 40G Interface: 2	Remove this	As per the ATC document point number n and o on page 5, It calls for only 1G and 10G interfaces. There is no mention of 40G interface. Hence the ask to remove it.	Cisco	As per ATC document
12	15.21	3	Storage Capacity (GB): 4,000 or higher	Storage Capacity (GB): 1800	for a 30G firewall. If daily log storage is even taken as 30Gb then it comes out to be 30*60=1800. Thus the ask to lower the number.	Cisco	Refer Corrigendum
13	15.31	3	Details of the Firewall Policies for the Firewall provided with the License: Web Security Essentials/URL Filtering, IPS License, Application Visibility License, APT (Advance Persistent Threat) License (Anti Malware Protection, C& C attacks, Geo IP Protection, Zero Day Threat protection), Gateway Anti virus, Gateway Anti spam	Details of the Firewall Policies for the Firewall provided with the License :Web Security Essentials/URL Filtering, IPS License, Application Visibility License, APT (Advance Persistent Threat) License (Anti Malware Protection, C& C attacks, Geo IP Protection, Zero Day Threat protection).	Since Antimalware protection is already asked for in the RFP. Which also leverages anti-virus based static analysis capabilities to identify a threat. AV becomes redundant and hence the ask to remove it.	Cisco	Refer Corrigendum

14	16 (c)	4	SDWAN / multi-link load balancing facility	Multi-link load balancing/Load Sharing facility	SDWAN is a routing capability and not a firewall security feature. Also on Firewall Load Balancing and Sharing our used interchangeably. Hence the request for change.	Cisco	Additional Load balancer can be added for multilink
15	16 (f)	4	Sandbox: There should be separate appliance for zero day / sandbox / ATP with minimum 4x 1 GE SFP and 4 x RJ 45, 2x2 TB storage on-appliance in RAID 1, minimum 20 VMs support, VM sandboxing throughput of minimum 1,000 file per hour and sniffer throughput of 2 Gbps and should have all Win / Linux OS (which are not out of support) and MS office licenses from day 1. In case of appliance failure, there should be provision of HA appliance for redundancy with equivalent sandboxing throughput of 1,000 files per hour.	Sandbox: There should be separate appliance for zero day / sandbox / ATP with minimum 2x 10 GE SFP+ and 2 x RJ 45, 2x2 TB storage on-appliance in RAID 1, minimum 20 VMs support, VM sandboxing throughput of minimum 1,000 file per day should have all Win / Linux OS (which are not out of support) and MS office licenses from day 1. In case of appliance failure, there should be provision of HA appliance for redundancy with equivalent sandboxing throughput of 1,000 files per day	Since sandbox will be deployed out of band and not inline. Thus having 2*10G and 2*1G interface would provide all the necessary connectivity and hence the request to remove it. Also only unique files needs to be scanned and not every file because at the network level you cannot hold onto files while the files are being analysed. Thus the request for change.	Cisco	Refer Corrigendum
16	16 (j)	4	Automatic real-time signature generation within 5 minutes without human intervention.	Remove this	Specific to an OEM, Hence needs to be removed. This automatic real time signature doesn't work in practical because on a perimeter firewall before anything is deployed. It needs to be validated beforehand. Thus making it of no use.	Cisco	Refer Corrigendum
17	15.21	3	Storage Capacity (GB): 4,000 or higher	Any value	In the pretender meeting it was discussed that storage of 4 TB will be provided by DGR where OEM will provide the software & license for centralize management and logging	Forcepoint	Refer Corrigendum

18	15.31	3	Details of the Firewall Policies for the Firewall provided with the License: Web Security Essentials/URL Filtering, IPS License, Application Visibility License, APT (Advance Persistent Threat) License (Anti Malware Protection, C& C attacks, Geo IP Protection, Zero Day Threat protection), Gateway Anti virus, Gateway Anti spam	Web Security Essentials/URL Filtering, IPS License, Application Visibility License, APT (Advance Persistent Threat) License (Anti Malware Protection, C& C attacks, Geo IP Protection, Zero Day Threat protection), Gateway Anti virus	Anti SPAM is a dedicated separate solution, which could be the part of UTM but is not a function of NGFW which is designed for performance on a high performance demanding environment	Forcepoint	Refer Corrigendum
19	16 (f)	4	Sandbox: There should be separate appliance for zero day / sandbox / ATP with minimum 4x 1 GE SFP and 4 x RJ 45, 2x2 TB storage on-appliance in RAID 1, minimum 20 VMs support, VM sandboxing throughput of minimum 1,000 file per hour and sniffer throughput of 2 Gbps and should have all Win / Linux OS (which are not out of support) and MS office licenses from day 1. In case of appliance failure, there should be provision of HA appliance for redundancy with equivalent sandboxing throughput of 1,000 files per hour.	There should be separate appliance for zero day / sandbox / ATP which should support for 8000 files a day processing. Should include microsoft licenses from day 1, there should be provision of HA appliance for redundancy with equivalent sandboxing throughput	This point was already discussed in the pretender meeting that asking for these specs making it tilted to a single OEM and as agreed by all OEM that a single measure will be publish which is files a day count approx 10 where all OEMs were agreed. As not all files go to APT , these are very limited files which are unknown goes for sandboxing	Forcepoint	Refer Corrigendum
20	16 (g)	4	DNS sinkholing / trap / filtering / IP reputation and DNS threat feeds for malicious DNS request from inside hosts to outside bad domains / IP addresses and integrate and query third party external threat intelligence databases to block bad IP addresses, domains and URLs.	DNS sinkholing / trap / filtering / IP reputation and DNS threat feeds for malicious DNS request from inside hosts to outside bad domains / IP addresses and integrate and query third party external threat intelligence databases to block bad IP addresses, domains and URLs if the same intelligence is not the part of their own threat research labs	Some OEM does third party integration as if they don't do research by their own feeds, OEMs who already have strong intelligence lab will provide their own feeds to the devices, not all OEM offer third party threat feeds	Forcepoint	As per ATC document

21	16 (j)	4	Automatic real-time signature generation within 5 minutes without human intervention.	Automatic real-time signature generation without human intervention.	OEM specific clause. Also time depends on the execution of malware which depends on the malware content.	Forcepoint	Refer Corrigendum
22	16 (l)	5	Support for NAT64, DHCPv6 and DNS64.	Support for NAT , PAT and IPv6 ready	This was already discussed in the pretender meeting that this function is of no use for DGR environment and it can be done using other technologies like load balancers, Pls allow our participation as this is also in our road map of 2020	Forcepoint	Refer Corrigendum
23	16 (o)	5	10G SFP+ interface should also support 1 GE SFP.	Request you to remove this clause	No all major OEMS support this compatibility , technology limitation, you may ask separate modules to be provided which can be replaced with the existing modules	Forcepoint	As per ATC document
24	NA	NA	New Point	Security effectiveness in NSS lab latest/retest report should be more then 99% and should not have observed any evasion	We have discussed this requirement in the pretender meeting where all major OEMs were agreed	Forcepoint	Not required
25	15.3	2	Features: Layer 3-Layer 4 NAT, VPN, Application Visibility and Control (AVC), User Identify, Next Generation Intrusion Prevention System (IPS), Zero Day Protection / Advance Malware Protection, Web Security Essentials / URL filtering	Layer 3-Layer 4 NAT, VPN, Application Visibility and Control (AVC), User Identify, Next Generation Intrusion Prevention System (IPS)	Not provided	Fortinet	As per ATC document
26	15.6	2	Throughput with all features (Real World/Prod Performance) (Under Test Condition (Mbps): 30,000 or higher	If it is Threat Prevention throughput than it should be lower than NGFW throughput around 20 Gbps	Not provided	Fortinet	As per ATC document

27	15.7	2	Throughput (Real World/Prod Performance) (Under Test Condition (Mbps): 30,000 or higher	This NGFW as asked on additional terms & conditions.	Not provided	Fortinet	Refer Corrigendum. Clause stands deleted. Accordingly, any value would be accepted.
28	15.25	3	Hot Swappable (Redundant Fan)	No We Don't have Hot Swapable Fan, We can replace the entire hardware incase of Fan failure.	Not provided	Fortinet	Refer Corrigendum
29	15.29	3	Interface Expansion slots supported: 2	We have fix architecture and we can provide till 100G from Day One.	Not provided	Fortinet	Refer Corrigendum
30	15.36	4	Maximum Operating Temperature (Degree C): 50	Changes requested till 40	Not provided	Fortinet	Refer Corrigendum
31	15.37	4	Minimum Operating Humidity (%RH): 5	Changes requested till 10	Not provided	Fortinet	Refer Corrigendum
32	16 (f)	4	Sandbox: There should be separate appliance for zero day / sandbox / ATP with minimum 4x 1 GE SFP and 4 x RJ 45, 2x2 TB storage on-appliance in RAID 1, minimum 20 VMs support, VM sandboxing throughput of minimum 1,000 file per hour and sniffer throughput of 2 Gbps and should have all Win / Linux OS (which are not out of support) and MS office licenses from day 1. In case of appliance failure, there should be provision of HA appliance for redundancy with equivalent sandboxing throughput of 1,000 files per hour.	Sandbox: There should be separate appliance for zero day / sandbox / ATP with minimum 4 x RJ 45 and 2x 10 GE SFP+, 2x2 TB storage on-appliance in RAID 1, minimum 20 VMs support, Real-world Effective Throughput of minimum 1,000 file per hour and sniffer throughput of 2 Gbps and should have Windows 7, Windows 8, Windows 10, macOS, Linux and Android (which are not out of support) and MS office licenses from day 1. In case of appliance failure, there should be provision of HA appliance for redundancy with equivalent Real-world Effective Throughput of 1,000 files per hour.	Not provided	Fortinet	Refer Corrigendum

33	16 (p)	5	In addition to the storage capacity, offloading and uploading facility should be available over SAN.	In addition to the storage capacity, log uploading facility should be available over FTP, SFTP, or SCP.	Not provided	Fortinet	Refer Corrigendum