पंजाब नैशनल बैंक ...भरोसे का प्रतीक ! punjab national bank ...the name you can BANK upon !

Information Technology Division, HO, 5, Sansad Marg, New Delhi – 110 001

Email: itdhw@pnb.co.in Tel: 011-23311452

Response to Queries: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component.

Sl No.	RFP Page Number	RFP Clause & Number	RFP Clause	Bidder's Query	Response
1.	149	**Scoring Methodology (S No 1)**	No. of Implementations of Designing of Information Security architecture/ System Integration of IT Security solution/ Information security components/SOC in India in Schedule Public Sector Banks/ Schedule Private Sector Banks/ Schedule Foreign Banks in India in last 5 years (from RFP Submission date) for Security Solutions by the Bidder. **(5 Marks)**	We assume that under SoC **(SOAR or SIEM)** management reference should be accepted with **5 marks.**	SOAR and SIEM are considered to be part of Security Operation Centre component for this clause in the RFP
2.	149	**Scoring Methodology (S No 2)**	Bidder's experience of Designing of Information Security architecture/ System integration of IT Security solution/ Information security components/SOC in India in Scheduled Commercial Banks in India with minimum **2 Lakh crore business** (as on FY 2021-22 / FY 2020-21) (5 Marks)	We assume the references of Bank in India with minimum turnover of **INR 1.4 Lakhs Crore with SOAR or SIEM management** should be accepted with **5 marks**.	Please refer to the Corrigendum
3.	150	**Scoring Methodology S No 11**	Marks on resources experience – 1. 1 marks for minimum 10 CCIE/CISSP in the organisation on company payroll for experience of minimum 5 years. 2. 0.5 mark per CCIE/CISSP certified resource above 10 resources having experience of more than 5 years (Undertaking along with duly Bio Data of onsite resource experience to be submitted. Employee should be on company payroll). (5 Marks)	We assume that along with CCIE and CISSP, the **CISM candidates** references should also be accepted with **5 marks.**	Please be guided as per the RFP
4.	Page 37 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component	Throughput: Inspection and Mitigation: 20 Gbps	DDoS appliance is a transparent appliance and it should not be part of any stateful appliance. As per industry standard, DDoS sizing should be done based on inspection, mitigation and prevention rate.	Please be guided as per the RFP

		Anti DoS/ DDoS preventive module S. N. 33	DDoS Flood Attack Prevention Rate: Minimum 30 Mpps DDoS Cloud Mitigation: 4 Gbps	Appliance should have sufficient capacity to meet all the requirements. Mitigation throughput should always be doubled than Inspected throughput. Attack Prevention Rate should be inline with the throughpt asked, it should not be undersized. DDoS appliance and Cloud should be from same OEM and both should be in sync including attack footprints to mitigate attack effectively. Cloud Scrubbing should be based out of India. It should not have any limitation in handling attack traffic and always ensure clean traffic of 4Gbps. **Suggested Clause: Throughput:** **Inspection Throughput: 30 Gbps** **Mitigation Throughput: 60 Gbps** **DDoS Flood Attack Prevention Rate: 40 Mpps** **DDoS Cloud Mitigation: 4 Gbps legitimate Appliance and scrubbing from same OEM and both should be in sync including attack footprints. Scrubbing should be based in India and have capability to handle unlimited attacks**	
5.	Page 37 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Anti DoS/ DDoS preventive module S. N. 34	Throughput Scalability: Inspection and Mitigation: 40 Gbps (without additional hardware) Layer 4: 40 Gbps with 100 Million Hardware sync DDoS Flood Attack Prevention Rate: 35 Mpps without hardware change (This performance figure must be mentioned in public facing datasheet). DDoS Cloud Mitigation: 20 Gbps	DDoS appliance is a transparent appliance and it should not be part of any stateful appliance, it should have capability to detect and mitigate L3-7 attacks. There should not be any limitation on handling attack concurrent sessions. As per industry standard, DDoS sizing should be done based on inspection, mitigation and prevention rate. Solution should be sufficient scalable to handle all the requirements. **Suggested Clause:**	Please be guided as per the RFP

				Throughput: **Inspection Throughput: 60 Gbps Mitigation Throughput: 120 Gbps Attack Concurrent Sessions: Unlimited DDoS Flood Attack Prevention Rate: 100 Mpps without hardware change (This performance figure must be mentioned in public facing datasheet). DDoS Cloud Mitigation: 20 Gbps legitimate**	
6.	Page 38 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Anti DoS/ DDoS preventive module S. N. 37	Ports: 8X 10G ports (SFP + Fiber port), 4x 40G (QSFP + Fiber port) ports 2 x 1G RJ45 Management Port . Fail to wire switch along with proposed device with minimum 4 bypass segment/ or can be achieved through additional external switch populated with same interfaces capacity to achieve fail over or Achieved through software by pass at interface level	Appliance should have sufficient port to cater current and future requirements. **Suggested Clause: Ports:** **12 X 10G ports (SFP + Fiber port), 8 x 40G (QSFP + Fiber port) ports 2 x 1G RJ45 Management Port and dedicated RJ45 Console Port Fail to wire switch along with proposed device with minimum 4 bypass segment/ or can be achieved through additional external switch populated with same interfaces** **capacity to achieve fail over or Achieved through software by pass at interface level**	Please refer to the Corrigendum
7.	Page 38 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Anti DoS/ DDoS preventive module S. N. 40	Bidder has to provide threat intel solution from the OEMs of proposed systems for internal device consumption, in addition to the same bidder has to provide third party dedicated Threat Intelligence Feed from reputed OEMs. Third party Threat Intelligence Feed should able to provide analysis report/network graph analysis relation report based on historical data of the threat actor, threat activity, threat objects (historical data of the IPs, URLs, etc. used by the malicious entity, actors involved in the past incidences around the world), exploits run from the detected IPs, provide extensive context and malware analysis in addition to the threat indicators and any	Leading OEM have their own threat intelligence feed to detect and mitigate TOR, Reputation, IOC and Active Attackers based blocking and keep the system attacker free. **Suggested Clause: Bidder has to provide threat intel solution from the OEMs of proposed systems to detect and mitigate TOR, Reputation, IOC and Active Attackers based blocking.**	Please refer to the Corrigendum

			other valuable information. Search option should be available for minimum 5 analysts. Bidder has to factor necessary hardware/software/database etc for hosting above system in DC and DR if required. External threat intelligence system should be from renowned OEMs.	**Threat intelligence system should be from renowned OEMs.**	
8.	Page 38 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Anti DoS/ DDoS preventive module S. N. 41	The DDOS Appliance should support inbuilt Threat intelligence Gateway (TIG) feature for outbound threat blocking and should support third party threat feeds in industry standard STIX & TAXII format.	OEM should have its own threat intelligence feed to block malicious threats. **Suggested Clause:** **The solution should support threat intelligence feed to block inbound/outbound threat**	Please refer to the Corrigendum
9.	Page 38 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Anti DoS/ DDoS preventive module S. N. 42	Proposed product/solution should be stateless Technology not having any kind of state limitation e.g. TCP connections	As appliance asked is stateless in nature it should be able to handle unlimited attack concurrent sessions to avoid bottleneck in case of large attacks.It should not be part of any statefull appliance. **Suggested Clause:** **Proposed product/solution should be stateless Technology not having any kind of state limitation e.g. TCP connections It should have capability to handle unlimited attack concurrent sessions.**	Please be guided as per the RFP
10.	Page 39 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Anti DoS/ DDoS preventive module S. N. 48	a)Inbuilt mechanism to inspect traffic with external threat feed and shall support at least 3Million IOC's for inline blocking (URL, domain and IP address subnet) b)OPTIONAL: The solution has Inbuilt mechanism to inspect traffic with external threat intelligence feed and shall support at least 3Million hash for inline blocking	Leading OEM have their own threat intelligence feed to detect TOR, IP Reputation, IOC blocking. **Suggested Clause:** **a)Inbuilt mechanism to inspect traffic with threat feeds (TOR, IP Reputation and IOC blocking)** **b)OPTIONAL: The solution has Inbuilt mechanism to inspect traffic with external threat intelligence feed and shall support at least 3Million hash for inline blocking**	Please refer to the Corrigendum

11.	Page 39 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Anti DoS/ DDoS preventive module S. N. 51	Support integration of external Threat Intelligence Platform (TIP) and Support Threat Intelligence Feed	Leading OEM have their own threat intelligence feed to detect malicious threats in real time. **Suggested Clause: Support Threat Intelligence Feed**	Please refer to the Corrigendum
12.	Page 39 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Anti DoS/ DDoS preventive module S. N. 62	Support comprehensive countermeasure to protect against zero-day attack, Challenge - Response Mechanism, and which should be able to Detect and protect attacks in real time through inbuilt Captcha Mechanism or HTTP Authentication	Every OEM has its own method to detect and mitigate attacks, one method should not get higher marks verses other. Functionality should be supported. **Suggested Clause: Support comprehensive countermeasure to protect against zero-day attack, Challenge - Response Mechanism, and which should be able to Detect and protect attacks in real time through inbuilt Captcha Mechanism or HTTP Authentication or Equivalent. Equal marks for each method - Supports CAPTCHA- 5Marks (Max) Supports HTTP – 5Marks Supports(Equivalent)-5Marks**	Please refer to the Corrigendum
13.	Page 40 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Anti DoS/ DDoS preventive module S. N. 71	Inspect SSL traffic for both RSA and ECC base key. Device should have support minimum 100,000 SSL TPS without session reuse for ECC & 2048 key RSA from day one and scalable up to 200,000 SSL TPS without hardware change	Appliance should not be oversized, it will unneccessary increase the overall cost. **Suggested Clause: Inspect SSL traffic for both RSA and ECC base key. Device should have support minimum 100,000 SSL TPS without session reuse for 2K key from day one and scalable up to 140,000 SSL TPS without hardware change. Key less functionality should also be supported.**	Please refer to the Corrigendum
14.	Page 42 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber	Bandwidth should be dedicated and not shared. Connectivity required, if any, will have to be arranged and factored by the bidder.	OEM should ensure Clean bandwidth should be available always for the PNB. **Suggested Clause:**	Please refer to the Corrigendum

		Security Component Anti DoS/ DDoS preventive module S. N. 104		**OEM should provide scrubbing to mitigate unlimited attacks and ensure required legitimate throughput should always be available for PNB**	
15.	Page 43 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Network Intrusion Prevention System (NIPS) S. N. 111	Ports: Minimum of 4X10G copper ports with fail open and 6X40G QSFP+ fiber ports with fail open Dedicated 1 (1G / 100M) port for management console	As appliances has been asked in HA, fail-open is not required. Software fail-open can be considered like we have considered in DDoS. Sufficient SFP+ ports should be asked and it should not be copper port to cater current and future requirements. NIPS are transparent appliance, it should not be part of any statefull architecture and should not have any limitation on handling attack sessions. Only way to manage this appliance is through management port which should be redundant to avoid bottleneck in case of port failure, same has been considered for DDoS. Suggested Clause: **Ports:** **Minimum of 12X10G SFP+ and 8X40G QSFP+ fiber ports with software bypass Dedicated 2 (1G / 100M) port for management and RJ45 for console** **Appliance should be transparent and should not be part of any statefull appliance with unlimited attack concurrent session handling.**	Please be guided as per the RFP
16.	Page 44 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Network Intrusion Prevention System (NIPS) S. N. 117	High availability in Active-active and active-passive mode with stateful failover and not only limited to transparent mode.	NIPS should always be transparent and stateless in nature to avoid bottleneck in case of attacks, appliance should not be visible to the attackers. **Suggested Clause:** **Support High availability with transparent and stateless in nature.**	Please be guided as per the RFP

17.	Page 44 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Network Intrusion Prevention System (NIPS) S. N. 132	Support Active-Active High Availability. It should support stateful HA such that state information is shared between the HA appliance. In case one of the appliances fails state is maintained. The HA should be out of the box solution and should not require any third party or additional software for the same	NIPS should always be transparent and stateless in nature, it can't host ip address on its interfaces. Hence, third pary is required for HA. **Suggested Clause: Support High Availability**	Please be guided as per the RFP
18.	Page 56 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Application Delivery Controller (ADC) with Threat Intelligence Gateway and SSL/TLS Offloader S. N. 264	CPU: 24 Physical Cores	12 Core CPU is sufficient to met the technical requirement, appliance should not be oversized. ADC appliance should be purpose built dedicated applliance. **Suggested Clause: CPU:** **12 Core**	Please be guided as per the RFP
19.	Page 56 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Application Delivery Controller (ADC) with Threat Intelligence Gateway and SSL/TLS Offloader S. N. 265	RAM: 256 GB	96GB RAM is sufficient to met the technical requirement, scalability should be considered. ADC appliance should be purpose built dedicated applliance. **Suggested Clause: RAM:** **96GB and scalable upto 192GB**	Please be guided as per the RFP
20.	Page 56 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Application Delivery Controller (ADC) with Threat Intelligence Gateway and SSL/TLS	Throughput: L7: 150 Gbps L7 requests:4.5M L4 requests:1.5M SSL TPS:100000 RSA 2048-bit keys SSL TPS: 90000 ECDSA P-256-bit	Appliance should not be oversized, it will unneccessary increase the overall cost. **Suggested Clause: Throughput:** **L4: 150 Gbps** **L7 requests:3M** **L4 requests:1.5M**	Please be guided as per the RFP

		Offloader S. N. 267		**SSL TPS:60000 RSA 2048-bit keys** **SSL TPS: 30000 ECDSA P-256-bit**	
21.	Page 56 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Application Delivery Controller (ADC) with Threat Intelligence Gateway and SSL/TLS Offloader S. N. 268	Throughput Scalability (without any additional hardware): L7: 175 Gbps L7 requests:6.5M L4 requests:2.5M SSL TPS: 200,000 RSA 2048-bit keys SSL TPS: 125,000 ECDSA P-256-bit	Appliance should not be oversized, it will unneccessary increase the overall cost. **Suggested Clause: Throughput:** **L4: 175 Gbps** **L7 requests:4M** **L4 requests:2.5M** **SSL TPS: 100,000 RSA 2048-bit keys** **SSL TPS: 45,000 ECDSA P-256-bit**	Please be guided as per the RFP
22.	Page 57 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Application Delivery Controller (ADC) with Threat Intelligence Gateway and SSL/TLS Offloader S. N. 270	SSL Offloading: 60 Gbps Scalable upto 90 Gbps (without any additional hardware)	Appliance should not be oversized, it will unneccessary increase the overall cost. **Suggested Clause: SSL Offloading: 35 Gbps** **Scalable upto 45 Gbps (without any additional hardware)**	Please be guided as per the RFP
23.	Page 57 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Application Delivery Controller (ADC) with Threat Intelligence Gateway and SSL/TLS Offloader S. N. 271	Ports: 4*100G 16*25G	Appliance should not be oversized, it will unneccessary increase the overall cost. Management Port should be redundant to avoid port failure dependency. **Suggested Clause: Ports:** **2*100G** **16*25G** **Dedicated 2x1G RJ45 Management Port and RJ45 Console Port**	Please be guided as per the RFP

24.	Page 57 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Application Delivery Controller (ADC) with Threat Intelligence Gateway and SSL/TLS Offloader S. N. 272	Form Factor: 1RU (Preferably)	Hardware size should not restrict any OEM from Participation, 2RU should also be considered. **Suggested Clause:** **1RU/2RU (Preferably)**	Please refer to the Corrigendum
25.	Page 57 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Application Delivery Controller (ADC) with Threat Intelligence Gateway and SSL/TLS Offloader S. N. 273	Instances (Isolated): 20 scalable upto 35 (without any additional hardware)	Appliance should not be oversized, it will unneccessary increase the overall cost. **Suggested Clause:** **10 scalable upto 60 (without any additional hardware).** **Each instance should have dedicated Resource, Configuration, Management and Opertaing System.**	Please be guided as per the RFP
26.	Page 57 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Application Delivery Controller (ADC) with Threat Intelligence Gateway and SSL/TLS Offloader S. N. 274	The proposed solution as dedicated Hardware appliance based Next Generation Load Balancer, DNS, DNS Security and Global Server Load Balancing, Bot protection and API Security solution should be on single platform	There is a dedicated appliance has been asked to protect from DNS attacks, Bot and API protection. It should not be part of ADC. **Suggested Clause:** **The proposed solution as dedicated Hardware appliance based Next Generation Load Balancer, DNS and Global Server Load Balancing should be on single platform**	Please be guided as per the RFP
27.	Page 57 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Application Delivery Controller (ADC) with	The solution must support Reverse proxy or full proxy (Forward Proxy & Reverse Proxy) architecture for HTTP1.1 & HTTP/2 based application traffic. Support IPv6 for Reverse Proxy deployments, IPv4 to IPv6 and IPv6 to IPv4 Dual Stack communication. Device should have inbuilt SSL VPN capability for supporting users over VPN	There is a separate appliance has been asked to for VPN. It should not be part of ADC. **Suggested Clause:** **The solution must support Reverse proxy or full proxy (Forward Proxy & Reverse**	Please be guided as per the RFP

		Threat Intelligence Gateway and SSL/TLS Offloader S. N. 275		**Proxy) architecture for HTTP1.1 & HTTP/2 based application traffic. Support IPv6 for Reverse Proxy deployments, IPv4 to IPv6 and IPv6 to IPv4 Dual Stack communication.**	
28.	Page 57 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Application Delivery Controller (ADC) with Threat Intelligence Gateway and SSL/TLS Offloader S. N. 276	Always on management & LED to initial configuration	There should be dedicated redundant management port for management & reporting. Console Port should be used for initial configuration. LED should not be used for OEM restriction. **Suggested Clause:** **Always on management & console to initial configuration** **Dedicated 2x1G RJ45 Management Port and RJ45 Console Port**	Please refer to the Corrigendum
29.	Page 57 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Application Delivery Controller (ADC) with Threat Intelligence Gateway and SSL/TLS Offloader S. N. 281	Capability to imply individual SSL certificate based on back-end application and remote end users secure communication. The solution should support Industry Standard Central Certificate Server integration feature so that new SSL certificate will be automatically update from central certificate server if existing certificate is expired.	ADC appliance should maintain required certificate and key to achieve SSL Offloading. **Suggested Clause:** **Capability to imply individual SSL certificate based on back-end application and remote end users secure communication. Should support Front end as well as Backend SSL.**	Please be guided as per the RFP
30.	Page 59 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component SSL Inspection S. N. 301	CPU: 24 Physical Cores	12 Core CPU is sufficient to met the technical requirement, appliance should not be oversized. ADC appliance should be purpose built dedicated appliiance. **Suggested Clause:** **CPU:** **12 Core**	Please be guided as per the RFP
31.	Page 59 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and	Storage:	Log will be stored in smaller in size on an appliance whereas centralized management stores all the data required for reporting.	Please be guided as per the RFP

		Management of Cyber Security Component SSL Inspection S. N. 302	Minimum 2x 1TB U.2 Enterprise-class SSD (RAID 1 Mirrored)	Hence, 500GB SSD is sufficient for storage log on an appliance, same sizing has been cosidered for other components as well. **Suggsted Clause: Storage:** **Minimum 500GB SSD**	
32.	Page 59 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component SSL Inspection S. N. 303	RAM: Minimum 256 GB	96GB RAM is sufficient to met the technical requirement, scalability should be considered. ADC appliance should be purpose built dedicated applliance. **Suggested Clause: RAM:** **96GB and scalable upto 192GB**	Please be guided as per the RFP
33.	Page 59 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component SSL Inspection S. N. 304	Power on demand: Dual AC/DC supply with hot swappable units, with always on management & LED to initial configuration	There should be dedicated redundant management port for management & reporting. Console Port should be used for intial configuration. LED should not be used for OEM restriction. **Suggested Clause: Dual AC/DC supply with hot swappable units, with always on management & console to initial configuration Dedicated 2x1G RJ45 Management Port and RJ45 Console Port**	Please refer to the Corrigendum
34.	Page 59 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component SSL Inspection S. N. 306	4*100G ports and 16*25G/10G with negotiable to 10G with SFP+/ QSFP+ as per the compatible interfaces	Appliance should not be oversized, it will unneccessary increase the overall cost. Management Port should be redundant to avoid port failure dependency. **Suggested Clause: Ports:** **2*100G ports and 16*25G/10G with negotiable to 10G with SFP+/ QSFP+ as per the compatible interfaces**	Please be guided as per the RFP

				Dedicated 2x1G RJ45 Management Port and RJ45 Console Port	
35.	Page 60 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component SSL Inspection S. N. 309	Should support 200K SSL TPS of 2048 key size. Device should support both L2 and L3 deployment with ICAP support	Appliance should not be oversized, it will unneccessary increase the overall cost. ECC Cipher support should also be considered. **Suggested Clause: Should support 100K SSL TPS of 2048 key size and 45K SSL TPS of EC-P256. Device should support both L2 and L3 deployment. ICAP support should also be available on proposed solution.**	Please be guided as per the RFP
36.	Page 60 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component SSL Inspection S. N. 310	Device should provide ADC functionality as mentioned in RFP and should support virtualization.	The proposed device should support next generation features like Virtualization that can that virtualizes the Device resources—including CPU, memory, network, acceleration resources, Operating system to provide complete separate environment from applications and management perspective. Even if one virtual instance is rebooted it should not impact the other instances running on the same hardware. **Suggested Clause : Device should provide ADC functionality and should support next generation features like Virtualization that virtualizes the Device resources—including CPU, memory, network, operating system, and acceleration resources. Appliance should support virtualized as well as standalone mode.** **Each virtual ADC instance contains a complete and separated environment of the Following:** **a) Resources, b) Configurations, c) Management, d) Operating System** **Appliance should support 10vADC from day1 and scalable upto 50vADC.**	Please be guided as per the RFP

37.	Page 60 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component SSL Inspection S. N. 311	L7 throughput of device should be minimum 180 Gbps	Appliance should not be oversized, it will unneccessary increase the overall cost. **Suggested Clause:** **L4 throughput of device should be minimum 180 Gbps**	Please be guided as per the RFP
38.	Page 60 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component SSL Inspection	New Clause Request	Filtering the traffic based on requirement should be part of SSL Inspection solution, it will ensure only the required traffic will be inspected and remaining will be bypassed. **Suggested Clause:** **Appliance should have URL filtering feature available**	Please be guided as per the RFP
39.	Page 60 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Web Application Firewall (WAF) S. N. 314	CPU: 24 Physical Cores	12 Core CPU is sufficient to met the technical requirement, appliance should not be oversized. ADC appliance should be purpose built dedicated applliance. **Suggested Clause:** **CPU:** **12 Core**	Please be guided as per the RFP
40.	Page 60 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Web Application Firewall (WAF) S. N. 315	RAM: 256 GB	96GB RAM is sufficient to met all the technical requirement, scalability should be considered. Appliance should not be oversized. **Suggested Clause:** **RAM:** **96 GB and scalable upto 192GB**	Please be guided as per the RFP
41.	Page 60 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Web Application Firewall	Form Factor: 1RU (Preferably)	Hardware size should not restrict any OEM from Participation, 2RU should also be considered. **Suggested Clause:**	Please refer to the Corrigendum

		(WAF) S. N. 321		**1RU/2RU (Preferably)**	
42.	Page 60 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Web Application Firewall (WAF) S. N. 322	Ports: 4*100G ports and 16*25G/10G with negotiable to 10G with SFP+/ QSFP+ as per the compatible interfaces	Appliance should not be oversized, it should have sufficient port to cater current and future requirements. Management port should be redundant to isolate port failure dependency. **Suggested Clause:** **Ports:** **2*100G ports and 16*25G/10G with negotiable to 10G with SFP+/ QSFP+ as per the compatible interfaces Dediacted 2x1G RJ45 Management Port and RJ45 Console Port**	Please be guided as per the RFP
43.	Page 63 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Web Application Firewall (WAF) S. N. 360	a) Automatically update Certificate bundles from the appropriate CAs without any user intervention OR b) Appliance should maintain certificate and key repository	WAF should host certificate and key for an application to decrypt and inspect mallicius contect over secure channel https. Auto upadte of certifcate should not be part of WAF. **Suggested Clause.** **Appliance should maintain certificate and key repository**	Please be guided as per the RFP
44.	Page 65 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Web Application Firewall (WAF) S. N. 377	The solution should provide online troubleshooting and traffic analysis tool where customer can take snapshot of appliance configuration and upload it on OEM's web based diagnostic tool to check the health and vulnerability of appliance with recommended solution provided on knowledge base link	Troubleshooting and analysis should be done offline with the help of TAC or onsite resource. OEM provides online site for knowledge and learning. **Suggested Clause:** **The solution should provide troubleshooting and traffic analysis. Proposed OEM should have dedicated online portal for knowledge and learning.**	Please refer to the Corrigendum
45.	Page 67 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and	New Clause Request	Certification like ICSA, NSS and PCI-DSS is very important to choose right WAF solution, it will ensure right protection has been	Please be guided as per the RFP

		Management of Cyber Security Component Web Application Firewall (WAF) S. N. 377		choosen to mitigate sophesticated attacks. **Suggested Clause:** **The WAF should be ICSA certified, NSS Lab Recommended and PCI Compliant**	
46.	Page 67 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Web Application Firewall (WAF) S. N. 377	New Clause Request	The proposed device should support next generation features like Virtualization that can that virtualizes the Device resources— including CPU, memory, network, acceleration resources, Operating system to provide complete separate environment from applications and management perspective. Even if one virtual instance is rebooted it should not impact the other instances running on the same hardware. **Suggested Clause :** **The proposed Appliance should be dedicated hardware to support next generation features like Virtualization that virtualizes the Device resources— including CPU, memory, network, operating system, and acceleration resources.** **Each virtual ADC instance contains a complete and separated environment of the Following:** **a) Resources, b) Configurations, c) Management, d) Operating System Appliance should support 10vADC from day1 and scalable upto 50vADC.**	Please be guided as per the RFP
47.	Page 67 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Web Application Firewall (WAF) S. N. 377	New Clause Request	WAF should have capability to send signal to DDoS to stop attacks at parameter itself, Attacker will not reach to WAF then. **Suggested Clause:** **Proposed WAF and DDoS Should integrate with each other. It should have a unique Messaging mechanism that efficiently mitigates attacks by sending**	Please be guided as per the RFP

				attack information to DDoS located at the Network Perimeter.	
48.	Page 76 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Network Load Balancer(NLB), Global Site Load Balancer(GSLB) external Application Delivery Controller (ADC) S. N. 498	CPU: 24 Core	12 Core CPU is sufficient to met all the technical requirement, appliance should not be oversized. ADC appliance should be purpose built dedicated appliance. **Suggested Clause: CPU:** **12 Core**	Please be guided as per the RFP
49.	Page 76 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Network Load Balancer(NLB), Global Site Load Balancer(GSLB) external Application Delivery Controller (ADC) S. N. 500	RAM: 256GB	96GB RAM is sufficient to met the technical requirement, scalability should be considered. **Suggested Clause: RAM:** **96 GB and scalable upto 192GB**	Please be guided as per the RFP
50.	Page 76 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Network Load Balancer(NLB), Global Site Load Balancer(GSLB) external Application Delivery Controller (ADC) S. N. 505	Ports: (4X40GE QSFP+ SR4 or 4X100GE SFP+ Ports) and (8X10GE SFP+ ports) SFP+/QSFP+ 1X1G Management port All ports should be fully populated	Appliance should not be oversized, it will unneccessary increase the overall cost without any specific requirement. Management Port should be redundant to avoid port failure dependency. **Suggested Clause: Ports:** **(4X40GE QSFP+ SR4 or 2X100GE SFP+ Ports)** **and** **(8X10GE SFP+ ports) SFP+/QSFP+ Dedicated 2x1G RJ45 Management Port**	Please be guided as per the RFP

				and RJ45 Console Port **All ports should be fully populated**	
51.	Page 76 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Network Load Balancer(NLB), Global Site Load Balancer(GSLB) external Application Delivery Controller (ADC) S. N. 507	Virtual Instances 15, scalable to 20 with complete network & resource isolation	Appliance should not be oversized, it will unneccessary increase the overall cost. **Suggested Clause:** **10 scalable upto 50 (without any additional hardware).** **Each instance should have dedicated Resource, Configuration, Management and Opertaing System.**	Please be guided as per the RFP
52.	Page 77 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Network Load Balancer(NLB), Global Site Load Balancer(GSLB) external Application Delivery Controller (ADC) S. N. 518	The ADC shall be manageable by SSH , HTTP, HTTPS, API, Console	Secure channel should be used for authentication. **Suggested Clause:** **The ADC shall be manageable by SSH , HTTPS, API, Console**	Please refer to the Corrigendum
53.	Page 77 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Network Load Balancer(NLB), Global Site Load Balancer(GSLB) external Application Delivery Controller (ADC) S. N. 522	The proposed solution as dedicated Hardware appliance based Next Generation Load Balancer, DNS, DNS Security and Global Server Load Balancing, should be on single platform	There is a dedicated hardware DDOS has been asked to protect DNS attacks. Asking the same features again on ADC without any spcific requirement will unneccessary increase the overall cost. **Suggested Clause:** **The proposed solution as dedicated Hardware appliance based Next Generation Load Balancer, DNS and Global Server Load Balancing, should be on single platform**	Please be guided as per the RFP

54.	Page 77 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Network Load Balancer(NLB), Global Site Load Balancer(GSLB) external Application Delivery Controller (ADC) S. N. 523	The solution must support Reverse proxy or full proxy (Forward Proxy & Reverse Proxy) architecture for HTTP1.1 & HTTP/2 based application traffic. Support IPv6 for Reverse Proxy deployments, IPv4 to IPv6 and IPv6 to IPv4 Dual Stack communication. Device should have inbuilt SSL VPN capability.	There is a dedicated solution for authentication/VPN has been asked in the RFP. Asking the same features again on ADC without any spcific requirement will unneccessary increase the overall cost. **Suggested Clause: The solution must support Reverse proxy or full proxy (Forward Proxy & Reverse Proxy) architecture for HTTP1.1 & HTTP/2 based application traffic. Support IPv6 for Reverse Proxy deployments, IPv4 to IPv6 and IPv6 to IPv4 Dual Stack communication**	Please refer to the Corrigendum
55.	Page 78 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Network Load Balancer(NLB), Global Site Load Balancer(GSLB) external Application Delivery Controller (ADC) S. N. 528	The solution must have ICAP integration with other security devices for file vulnerability, virus, Trojan scanning during file submission with webapplications to improve security or equivalent or built-in AV	ICAP integration can't be part of ADC with LB, it will unneccessary increase the overall cost without any specific requirement. **Suggested Clause: Delete the clause**	Please be guided as per the RFP
56.	Page 79 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Network Load Balancer(NLB), Global Site Load Balancer(GSLB) external Application Delivery Controller (ADC) S. N. 540	Supports DNS A, AAAA, A6, CNAME, DNAME, HINFO, KEY, MX, NS, NXT, PTR, SIG, SOA, SRV and TXR records	ADC should be a dedicated appliance, it should not work like a dedicated DNS server as it is already available in existing infra. **Suggested Clause: Appliance should be able to function as Authoritative Domain Name Server (ADNS), should be able to host AAAA Records, A Records and should also support DNSSEC**	Please be guided as per the RFP

57.	Page 37 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Anti DoS/ DDoS preventive module S. N. 33	Throughput: Inspection and Mitigation: 20 Gbps DDoS Flood Attack Prevention Rate: Minimum 30 Mpps DDoS Cloud Mitigation: 4 Gbps	DDoS appliance is a transparent appliance and it should not be part of any stateful appliance. As per industry standard, DDoS sizing should be done based on inspection, mitigation and prevention rate. Appliance should have sufficient capacity to meet all the requirements. Mitigation throughput should always be doubled than Inspected throughput. Attack Prevention Rate should be inline with the throughpt asked, it should not be undersized. DDoS appliance and Cloud should be from same OEM and both should be in sync including attack footprints to mitigate attack effectively. Cloud Scrubbing should be based out of India. It should not have any limitation in handling attack traffic and always ensure clean traffic of 4Gbps. **Suggested Clause: Throughput:** **Inspection Throughput: 30 Gbps** **Mitigation Throughput: 60 Gbps** **DDoS Flood Attack Prevention Rate: 40 Mpps** **DDoS Cloud Mitigation: 4 Gbps legitimate Appliance and scrubbing from same OEM and both should be in sync including attack footprints. Scrubbing should be based in India and have capability to handle unlimited attacks**	Please be guided as per the RFP
58.	Page 37 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Anti DoS/ DDoS preventive module S. N. 34	Throughput Scalability: Inspection and Mitigation: 40 Gbps (without additional hardware) Layer 4: 40 Gbps with 100 Million Hardware sync DDoS Flood Attack Prevention Rate: 35 Mpps without hardware change (This performance	DDoS appliance is a transparent appliance and it should not be part of any stateful appliance, it should have capability to detect and mitigate L3-7 attacks. There should not be any limitation on handling attack concurrent sessions. As per industry standard, DDoS sizing should be done based on inspection, mitigation and	Please be guided as per the RFP

			figure must be mentioned in public facing datasheet). DDoS Cloud Mitigation: 20 Gbps	prevention rate. Solution should be sufficient scalable to handle all the requirements. **Suggested Clause:** **Throughput:** **Inspection Throughput: 60 Gbps** **Mitigation Throughput: 120 Gbps** **Attack Concurrent Sessions: Unlimited** **DDoS Flood Attack Prevention Rate: 100 Mpps without hardware change (This performance figure must be mentioned in public facing datasheet).** **DDoS Cloud Mitigation: 20 Gbps legitimate**	
59.	Page 38 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Anti DoS/ DDoS preventive module S. N. 37	Ports: 8X 10G ports (SFP + Fiber port), 4x 40G (QSFP + Fiber port) ports 2 x 1G RJ45 Management Port . Fail to wire switch along with proposed device with minimum 4 bypass segment/ or can be achieved through additional external switch populated with same interfaces capacity to achieve fail over or Achived through software by pass at interface level	Appliance should have sufficient port to cater current and future requirements. **Suggested Clause:** **Ports:** **12 X 10G ports (SFP + Fiber port),** **8 x 40G (QSFP + Fiber port) ports** **2 x 1G RJ45 Management Port and dedicated RJ45 Console Port** **Fail to wire switch along with proposed device with minimum 4 bypass segment/ or can be achieved through additional external switch populated with same interfaces** **capacity to achieve fail over or Achived through software by pass at interface level**	Please refer to the Corrigendum
60.	Page 38 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Anti DoS/ DDoS	Bidder has to provide threat intel solution from the OEMs of proposed systems for internal device consumption, in addition to the same bidder has to provide third party dedicated Threat Intelligence Feed from reputed OEMs. Third party Threat Intelligence Feed should able to provide analysis report/network graph analysis relation report based on historical data of the threat actor, threat activity, threat objects (historical data of the IPs, URLs, etc. used by	Leading OEM have their own threat intelligence feed to detect and mitigate TOR, Ruputation, IOC and Active Attackers based blocking and keep the system attacker free. **Suggested Clause:** **Bidder has to provide threat intel solution**	Please refer to the Corrigendum

		preventive module S. N. 40	the malicious entity, actors involved in the past incidences around the world), exploits run from the detected IPs, provide extensive context and malware analysis in addition to the threat indicators and any other valuable information. Search option should be available for minimum 5 analysts. Bidder has to factor necessary hardware/software/database etc for hosting above system in DC and DR if required. External threat intelligence system should be from renowned OEMs.	**from the OEMs of proposed systems to detect and mitigate TOR, Ruputation, IOC and Active Attackers based blocking. Threat intelligence system should be from renowned OEMs.**	
61.	Page 38 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Anti DoS/ DDoS preventive module S. N. 41	The DDOS Appliance should support inbuilt Threat intelligence Gateway (TIG) feature for outbound threat blocking and should support third party threat feeds in industry standard STIX & TAXII format.	OEM should have its own threat intelligence feed to block mallicious threats. **Suggested Clause: The solution should support threat intelligence feed to block inbound/outbound threat**	Please refer to the Corrigendum.
62.	Page 38 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Anti DoS/ DDoS preventive module S. N. 42	Proposed product/solution should be stateless Technology not having any kind of state limitation e.g. TCP connections	As appliance asked is stateless in nature it should be able to handle unlimited attack concurrent sessions to avoid bottleneck in case of large attacks.It should not be part of any statefull appliance. **Suggested Clause: Proposed product/solution should be stateless Technology not having any kind of state limitation e.g. TCP connections It should have capability to handle unlimited attack concurrent sessions.**	Please be guided as per the RFP
63.	Page 39 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Anti DoS/ DDoS preventive module S. N. 48	a)Inbuilt mechanism to inspect traffic with external threat feed and shall support at least 3Million IOC's for inline blocking (URL, domain and IP address subnet) b)OPTIONAL: The solution has Inbuilt mechanism to inspect traffic with external threat intelligence feed and shall support at least 3Million hash for inline blocking	Leading OEM have their own threat intelligence feed to detect TOR, IP Ruputation, IOC blocking. **Suggested Clause:** **a)Inbuilt mechanism to inspect traffic with threat feeds (TOR, IP Reputation and IOC blocking)** **b)OPTIONAL: The solution has Inbuilt mechanism to inspect traffic with external**	Please refer to the Corrigendum.

				threat intelligence feed and shall support at least 3Million hash for inline blocking	
64.	Page 39 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Anti DoS/ DDoS preventive module S. N. 51	Support integration of external Threat Intelligence Platform (TIP) and Support Threat Intelligence Feed	Leading OEM have their own threat intelligence feed to detect mallicious threats in real time. **Suggested Clause: Support Threat Intelligence Feed**	Please refer to the Corrigendum.
65.	Page 39 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Anti DoS/ DDoS preventive module S. N. 62	Support comprehensive countermeasure to protect against zero-day attack, Challenge - Response Mechanism, and which should be able to Detect and protect attacks in real time through inbuilt Captcha Mechanism or HTTP Authentication	Every OEM has its own method to detect and mitigate attacks, one method should not get higher marks verses other. Functionality should be supported. **Suggested Clause: Support comprehensive countermeasure to protect against zero-day attack, Challenge - Response Mechanism, and which should be able to Detect and protect attacks in real time through inbuilt Captcha Mechanism or HTTP Authentication or Equivalent. Equal marks for each method - Supports CAPTCHA- 5Marks (Max) Supports HTTP – 5Marks Supports(Equivalent)-5Marks**	Please refer to the Corrigendum.
66.	Page 40 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Anti DoS/ DDoS preventive module S. N. 71	Inspect SSL traffic for both RSA and ECC base key. Device should have support minimum 100,000 SSL TPS without session reuse for ECC & 2048 key RSA from day one and scalable up to 200,000 SSL TPS without hardware change	Appliance should not be oversized, it will unneccessary increase the overall cost. **Suggested Clause: Inspect SSL traffic for both RSA and ECC base key. Device should have support minimum 100,000 SSL TPS without session reuse for 2K key from day one and scalable up to 140,000 SSL TPS without hardware change. Key less functionality should also be supported.**	Please refer to the Corrigendum.

67.	Page 42 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Anti DoS/ DDoS preventive module S. N. 104	Bandwidth should be dedicated and not shared. Connectivity required, if any, will have to be arranged and factored by the bidder.	OEM should ensure Clean bandwidth should be available always for the PNB. **Suggested Clause:** **OEM should provide scrubbing to mitigate unlimited attacks and ensure required legitimate throughput should always be available for PNB**	Please refer to the Corrigendum
68.	Page 43 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Network Intrusion Prevention System (NIPS) S. N. 111	Ports: Minimum of 4X10G copper ports with fail open and 6X40G QSFP+ fiber ports with fail open Dedicated 1 (1G / 100M) port for management console	As appliances has been asked in HA, fail-open is not required. Software fail-open can be considered like we have considered in DDoS. Sufficient SFP+ ports should be asked and it should not be copper port to cater current and future requirements. NIPS are transparent appliance, it should not be part of any statefull architecture and should not have any limitation on handling attack sessions. Only way to manage this appliance is through management port which should be redundant to avoid bottleneck in case of port failure, same has been considered for DDoS. Suggested Clause: **Ports:** **Minimum of 12X10G SFP+ and 8X40G QSFP+ fiber ports with software bypass Dedicated 2 (1G / 100M) port for management and RJ45 for console** **Appliance should be transparent and should not be part of any statefull appliance with unlimited attack concurrent session handling.**	Please be guided as per the RFP
69.	Page 44 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Network Intrusion	High availability in Active-active and active-passive mode with stateful failover and not only limited to transparent mode.	NIPS should always be transparent and stateless in nature to avoid bottleneck in case of attacks, appliance should not be visible to the attackers. **Suggested Clause:**	Please be guided as per the RFP

		Prevention System (NIPS) S. N. 117		**Support High availability with transparent and stateless in nature.**	
70.	Page 44 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Network Intrusion Prevention System (NIPS) S. N. 132	Support Active-Active High Availability. It should support stateful HA such that state information is shared between the HA appliance. In case one of the appliances fails state is maintained. The HA should be out of the box solution and should not require any third party or additional software for the same	NIPS should always be transparent and stateless in nature, it can't host ip address on its interfaces. Hence, third pary is required for HA. **Suggested Clause:** **Support High Availability**	Please be guided as per the RFP
71.	Page 56 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Application Delivery Controller (ADC) with Threat Intelligence Gateway and SSL/TLS Offloader S. N. 264	CPU: 24 Physical Cores	12 Core CPU is sufficient to met the technical requirement, appliance should not be oversized. ADC appliance should be purpose built dedicated applliance. **Suggested Clause:** **CPU:** **12 Core**	Please be guided as per the RFP
72.	Page 56 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Application Delivery Controller (ADC) with Threat Intelligence Gateway and SSL/TLS Offloader S. N. 265	RAM: 256 GB	96GB RAM is sufficient to met the technical requirement, scalability should be considered. ADC appliance should be purpose built dedicated applliance. **Suggested Clause:** **RAM:** **96GB and scalable upto 192GB**	Please be guided as per the RFP
73.	Page 56 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component	Throughput: L7: 150 Gbps L7 requests:4.5M L4 requests:1.5M	Appliance should not be oversized, it will unneccessary increase the overall cost. **Suggested Clause:** **Throughput:**	Please be guided as per the RFP

		Application Delivery Controller (ADC) with Threat Intelligence Gateway and SSL/TLS Offloader S. N. 267	SSL TPS:100000 RSA 2048-bit keys SSL TPS: 90000 ECDSA P-256-bit	**L4: 150 Gbps** **L7 requests:3M** **L4 requests:1.5M** **SSL TPS:60000 RSA 2048-bit keys** **SSL TPS: 30000 ECDSA P-256-bit**	
74.	Page 56 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Application Delivery Controller (ADC) with Threat Intelligence Gateway and SSL/TLS Offloader S. N. 268	Throughput Scalability (without any additional hardware): L7: 175 Gbps L7 requests:6.5M L4 requests:2.5M SSL TPS: 200,000 RSA 2048-bit keys SSL TPS: 125,000 ECDSA P-256-bit	Appliance should not be oversized, it will unneccessary increase the overall cost. **Suggested Clause: Throughput:** **L4: 175 Gbps** **L7 requests:4M** **L4 requests:2.5M** **SSL TPS: 100,000 RSA 2048-bit keys** **SSL TPS: 45,000 ECDSA P-256-bit**	Please be guided as per the RFP
75.	Page 57 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Application Delivery Controller (ADC) with Threat Intelligence Gateway and SSL/TLS Offloader S. N. 270	SSL Offloading: 60 Gbps Scalable upto 90 Gbps (without any additional hardware)	Appliance should not be oversized, it will unneccessary increase the overall cost. **Suggested Clause: SSL Offloading: 35 Gbps** **Scalable upto 45 Gbps (without any additional hardware)**	Please be guided as per the RFP
76.	Page 57 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Application Delivery Controller (ADC) with Threat Intelligence Gateway and SSL/TLS Offloader S. N. 271	Ports: 4*100G 16*25G	Appliance should not be oversized, it will unneccessary increase the overall cost. Management Port should be redundant to avoid port failure dependency. **Suggested Clause: Ports:** **2*100G** **16*25G**	Please be guided as per the RFP

				Dedicated 2x1G RJ45 Management Port and RJ45 Console Port	
77.	Page 57 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Application Delivery Controller (ADC) with Threat Intelligence Gateway and SSL/TLS Offloader S. N. 272	Form Factor: 1RU (Preferably)	Hardware size should not restrict any OEM from Participation, 2RU should also be considered. **Suggested Clause:** **1RU/2RU (Preferably)**	Please refer to the Corrigendum
78.	Page 57 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Application Delivery Controller (ADC) with Threat Intelligence Gateway and SSL/TLS Offloader S. N. 273	Instances (Isolated): 20 scalable upto 35 (without any additional hardware)	Appliance should not be oversized, it will unneccessary increase the overall cost. **Suggested Clause:** **10 scalable upto 60 (without any additional hardware).** **Each instance should have dedicated Resource, Configuration, Management and Opertaing System.**	Please be guided as per the RFP
79.	Page 57 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Application Delivery Controller (ADC) with Threat Intelligence Gateway and SSL/TLS Offloader S. N. 274	The proposed solution as dedicated Hardware appliance based Next Generation Load Balancer, DNS, DNS Security and Global Server Load Balancing, Bot protection and API Security solution should be on single platform	There is a dedicated appliance has been asked to protect from DNS attacks, Bot and API protection. It should not be part of ADC. **Suggested Clause:** **The proposed solution as dedicated Hardware appliance based Next Generation Load Balancer, DNS and Global Server Load Balancing should be on single platform**	Please be guided as per the RFP
80.	Page 57 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber	The solution must support Reverse proxy or full proxy (Forward Proxy & Reverse Proxy) architecture for HTTP1.1 & HTTP/2 based application traffic. Support IPv6 for Reverse Proxy deployments, IPv4 to IPv6 and IPv6	There is a separate appliance has been asked to for VPN. It should not be part of ADC.	Please be guided as per the RFP

		Security Component Application Delivery Controller (ADC) with Threat Intelligence Gateway and SSL/TLS Offloader S. N. 275	to IPv4 Dual Stack communication. Device should have inbuilt SSL VPN capability for supporting users over VPN	**Suggested Clause:** **The solution must support Reverse proxy or full proxy (Forward Proxy & Reverse Proxy) architecture for HTTP1.1 & HTTP/2 based application traffic. Support IPv6 for Reverse Proxy deployments, IPv4 to IPv6 and IPv6 to IPv4 Dual Stack communication.**	
81.	Page 57 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Application Delivery Controller (ADC) with Threat Intelligence Gateway and SSL/TLS Offloader S. N. 276	Always on management & LED to initial configuration	There should be dedicated redundant management port for management & reporting. Console Port should be used for intial configuration. LED should not be used for OEM restriction. **Suggested Clause:** **Always on management & console to initial configuration** **Dedicated 2x1G RJ45 Management Port and RJ45 Console Port**	Please refer to the Corrigendum.
82.	Page 57 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Application Delivery Controller (ADC) with Threat Intelligence Gateway and SSL/TLS Offloader S. N. 281	Capability to imply individual SSL certificate based on back-end application and remote end users secure communication. The solution should support Industry Standard Central Certificate Server integration feature so that new SSL certificate will be automatically update from central certificate server if existing certificate is expired.	ADC appliance should maintain required certificate and key to achieve SSL Offloading. **Suggested Clause:** **Capability to imply individual SSL certificate based on back-end application and remote end users secure communication. Should support Front end as well as Backend SSL.**	Please be guided as per the RFP
83.	Page 59 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component SSL Inspection S. N. 301	CPU: 24 Physical Cores	12 Core CPU is sufficient to met the technical requirement, appliance should not be oversized. ADC appliance should be purpose built dedicated applliance. **Suggested Clause:** **CPU:** **12 Core**	Please be guided as per the RFP

84.	Page 59 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component SSL Inspection S. N. 302	Storage: Minimum 2x 1TB U.2 Enterprise-class SSD (RAID 1 Mirrored)	Log will be stored in smaller in size on an appliance whereas centralized management stores all the data required for reporting. Hence, 500GB SSD is sufficient for storage log on an appliance, same sizing has been cosidered for other components as well. **Suggsted Clause: Storage:** **Minimum 500GB SSD**	Please be guided as per the RFP
85.	Page 59 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component SSL Inspection S. N. 303	RAM: Minimum 256 GB	96GB RAM is sufficient to met the technical requirement, scalability should be considered. ADC appliance should be purpose built dedicated appliance. **Suggested Clause: RAM:** **96GB and scalable upto 192GB**	Please be guided as per the RFP
86.	Page 59 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component SSL Inspection S. N. 304	Power on demand: Dual AC/DC supply with hot swappable units, with always on management & LED to initial configuration	There should be dedicated redundant management port for management & reporting. Console Port should be used for intial configuration. LED should not be used for OEM restriction. **Suggested Clause: Dual AC/DC supply with hot swappable units, with always on management & console to initial configuration Dedicated 2x1G RJ45 Management Port and RJ45 Console Port**	Please refer to the Corrigendum
87.	Page 59 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component SSL Inspection S. N. 306	4*100G ports and 16*25G/10G with negotiable to 10G with SFP+/ QSFP+ as per the compatible interfaces	Appliance should not be oversized, it will unneccessary increase the overall cost. Management Port should be redundant to avoid port failure dependency. **Suggested Clause: Ports:**	Please be guided as per the RFP

				2*100G ports and 16*25G/10G with negotiable to 10G with SFP+/ QSFP+ as per the compatible interfaces Dedicated 2x1G RJ45 Management Port and RJ45 Console Port	
88.	Page 60 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component SSL Inspection S. N. 309	Should support 200K SSL TPS of 2048 key size. Device should support both L2 and L3 deployment with ICAP support	Appliance should not be oversized, it will unneccessary increase the overall cost. ECC Cipher support should also be considered. **Suggested Clause: Should support 100K SSL TPS of 2048 key size and 45K SSL TPS of EC-P256. Device should support both L2 and L3 deployment. ICAP support should also be available on proposed solution.**	Please be guided as per the RFP
89.	Page 60 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component SSL Inspection S. N. 310	Device should provide ADC functionality as mentioned in RFP and should support virtualization.	The proposed device should support next generation features like Virtualization that can that virtualizes the Device resources—including CPU, memory, network, acceleration resources, Operating system to provide complete separate environment from applications and management perspective. Even if one virtual instance is rebooted it should not impact the other instances running on the same hardware. **Suggested Clause : Device should provide ADC functionality and should support next generation features like Virtualization that virtualizes the Device resources—including CPU, memory, network, operating system, and acceleration resources. Appliance should support virtualized as well as standalone mode.** **Each virtual ADC instance contains a complete and separated environment of the Following:** **a) Resources, b) Configurations, c) Management, d) Operating System**	Please be guided as per the RFP

				Appliance should support 10vADC from day1 and scalable upto 50vADC.	
90.	Page 60 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component SSL Inspection S. N. 311	L7 throughput of device should be minimum 180 Gbps	Appliance should not be oversized, it will unneccessary increase the overall cost. **Suggested Clause:** **L4 throughput of device should be minimum 180 Gbps**	Please be guided as per the RFP
91.	Page 60 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component SSL Inspection	New Clause Request	Filtering the traffic based on requirement should be part of SSL Inspection solution, it will ensure only the required traffic will be inspected and remaining will be bypassed. **Suggested Clause:** **Appliance should have URL filtering feature available**	Please be guided as per the RFP
92.	Page 60 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Web Application Firewall (WAF) S. N. 314	CPU: 24 Physical Cores	12 Core CPU is sufficient to met the technical requirement, appliance should not be oversized. ADC appliance should be purpose built dedicated applliance. **Suggested Clause:** **CPU:** **12 Core**	Please be guided as per the RFP
93.	Page 60 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Web Application Firewall (WAF) S. N. 315	RAM: 256 GB	96GB RAM is sufficient to met all the technical requirement, scalability should be considered. Appliance should not be oversized. **Suggested Clause:** **RAM:** **96 GB and scalable upto 192GB**	Please be guided as per the RFP
94.	Page 60 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and	Form Factor: 1RU (Preferably)	Hardware size should not restrict any OEM from Participation, 2RU should also be considered.	Please refer to the Corrigendum

		Management of Cyber Security Component Web Application Firewall (WAF) S. N. 321		**Suggested Clause:** **1RU/2RU (Preferably)**	
95.	Page 60 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Web Application Firewall (WAF) S. N. 322	Ports: 4*100G ports and 16*25G/10G with negotiable to 10G with SFP+/ QSFP+ as per the compatible interfaces	Appliance should not be oversized, it should have sufficient port to cater current and future requirements. Management port should be redundant to isolate port failure dependency. **Suggested Clause: Ports:** **2*100G ports and 16*25G/10G with negotiable to 10G with SFP+/ QSFP+ as per the compatible interfaces Dediacted 2x1G RJ45 Management Port and RJ45 Console Port**	Please be guided as per the RFP
96.	Page 63 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Web Application Firewall (WAF) S. N. 360	a) Automatically update Certificate bundles from the appropriate CAs without any user intervention OR b) Appliance should maintain certificate and key repository	WAF should host certificate and key for an application to decrypt and inspect mallicius contect over secure channel https. Auto upadte of certifcate should not be part of WAF. **Suggested Clause. Appliance should maintain certificate and key repository**	Please be guided as per the RFP
97.	Page 65 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Web Application Firewall (WAF) S. N. 377	The solution should provide online troubleshooting and traffic analysis tool where customer can take snapshot of appliance configuration and upload it on OEM's web based diagnostic tool to check the health and vulnerability of appliance with recommended solution provided on knowledge base link	Troubleshooting and analysis should be done offline with the help of TAC or onsite resource. OEM provides online site for knowledge and learning. **Suggested Clause:** **The solution should provide troubleshooting and traffic analysis. Proposed OEM should have dedicated online portal for knowledge and learning.**	Please refer to the Corrigendum

98.	Page 67 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Web Application Firewall (WAF) S. N. 377	New Clause Request	Certification like ICSA, NSS and PCI-DSS is very important to choose right WAF solution, it will ensure right protection has been choosen to mitigate sophesticated attacks. **Suggested Clause:** **The WAF should be ICSA certified, NSS Lab Recommended and PCI Compliant**	Please be guided as per the RFP
99.	Page 67 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Web Application Firewall (WAF) S. N. 377	New Clause Request	The proposed device should support next generation features like Virtualization that can that virtualizes the Device resources—including CPU, memory, network, acceleration resources, Operating system to provide complete separate environment from applications and management perspective. Even if one virtual instance is rebooted it should not impact the other instances running on the same hardware. **Suggested Clause :** **The proposed Appliance should be dedicated hardware to support next generation features like Virtualization that virtualizes the Device resources—including CPU, memory, network, operating system, and acceleration resources.** **Each virtual ADC instance contains a complete and separated environment of the Following:** **a) Resources, b) Configurations, c) Management, d) Operating System Appliance should support 10vADC from day1 and scalable upto 50vADC.**	Please be guided as per the RFP
100.	Page 67 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Web Application Firewall	New Clause Request	WAF should have capability to send signal to DDoS to stop attacks at parameter itself, Attacker will not reach to WAF then. **Suggested Clause:** **Proposed WAF and DDoS Should integrate with each other. It should have a**	Please be guided as per the RFP

		(WAF) S. N. 377		**unique Messaging mechanism that efficiently mitigates attacks by sending attack information to DDoS located at the Network Perimeter.**	
101.	Page 76 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Network Load Balancer(NLB), Global Site Load Balancer(GSLB) external Application Delivery Controller (ADC) S. N. 498	CPU: 24 Core	12 Core CPU is sufficient to met all the technical requirement, appliance should not be oversized. ADC appliance should be purpose built dedicated appliance. **Suggested Clause: CPU:** **12 Core**	Please be guided as per the RFP
102.	Page 76 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Network Load Balancer(NLB), Global Site Load Balancer(GSLB) external Application Delivery Controller (ADC) S. N. 500	RAM: 256GB	96GB RAM is sufficient to met the technical requirement, scalability should be considered. **Suggested Clause: RAM:** **96 GB and scalable upto 192GB**	Please be guided as per the RFP
103.	Page 76 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Network Load Balancer(NLB), Global Site Load Balancer(GSLB) external Application Delivery	Ports: (4X40GE QSFP+ SR4 or 4X100GE SFP+ Ports) and (8X10GE SFP+ ports) SFP+/QSFP+ 1X1G Management port All ports should be fully populated	Appliance should not be oversized, it will unneccessary increase the overall cost without any specific requirement. Management Port should be redundant to avoid port failure dependency. **Suggested Clause: Ports:** **(4X40GE QSFP+ SR4 or 2X100GE SFP+ Ports)** **and**	Please be guided as per the RFP

		Controller (ADC) S. N. 505		**(8X10GE SFP+ ports) SFP+/QSFP+ Dedicated 2x1G RJ45 Management Port and RJ45 Console Port All ports should be fully populated**	
104.	Page 76 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Network Load Balancer(NLB), Global Site Load Balancer(GSLB) external Application Delivery Controller (ADC) S. N. 507	Virtual Instances 15, scalable to 20 with complete network & resource isolation	Appliance should not be oversized, it will unneccessary increase the overall cost. **Suggested Clause: 10 scalable upto 50 (without any additional hardware). Each instance should have dedicated Resource, Configuration, Management and Opertaing System.**	Please be guided as per the RFP
105.	Page 77 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Network Load Balancer(NLB), Global Site Load Balancer(GSLB) external Application Delivery Controller (ADC) S. N. 518	The ADC shall be manageable by SSH , HTTP, HTTPS, API, Console	Secure channel should be used for authentication. **Suggested Clause: The ADC shall be manageable by SSH , HTTPS, API, Console**	Please refer to the Corrigendum
106.	Page 77 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Network Load Balancer(NLB), Global Site Load Balancer(GSLB) external Application Delivery	The proposed solution as dedicated Hardware appliance based Next Generation Load Balancer, DNS, DNS Security and Global Server Load Balancing, should be on single platform	There is a dedicated hardware DDOS has been asked to protect DNS attacks. Asking the same features again on ADC without any spcific requirement will unneccessary increase the overall cost. **Suggested Clause: The proposed solution as dedicated Hardware appliance based Next Generation Load Balancer, DNS and**	Please be guided as per the RFP

		Controller (ADC) S. N. 522		**Global Server Load Balancing, should be on single platform**	
107.	Page 77 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Network Load Balancer(NLB), Global Site Load Balancer(GSLB) external Application Delivery Controller (ADC) S. N. 523	The solution must support Reverse proxy or full proxy (Forward Proxy & Reverse Proxy) architecture for HTTP1.1 & HTTP/2 based application traffic. Support IPv6 for Reverse Proxy deployments, IPv4 to IPv6 and IPv6 to IPv4 Dual Stack communication. Device should have inbuilt SSL VPN capability.	There is a dedicated solution for authentication/VPN has been asked in the RFP. Asking the same features again on ADC without any spcific requirement will unneccessary increase the overall cost. **Suggested Clause:** **The solution must support Reverse proxy or full proxy (Forward Proxy & Reverse Proxy) architecture for HTTP1.1 & HTTP/2 based application traffic. Support IPv6 for Reverse Proxy deployments, IPv4 to IPv6 and IPv6 to IPv4 Dual Stack communication**	Please be guided as per the RFP
108.	Page 78 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Network Load Balancer(NLB), Global Site Load Balancer(GSLB) external Application Delivery Controller (ADC) S. N. 528	The solution must have ICAP integration with other security devices for file vulnerability, virus, Trojan scanning during file submission with webapplications to improve security or equivalent or built-in AV	ICAP integration can't be part of ADC with LB, it will unneccessary increase the overall cost without any specific requirement. **Suggested Clause:** **Delete the clause**	Please be guided as per the RFP
109.	Page 79 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Network Load Balancer(NLB), Global Site Load Balancer(GSLB) external Application Delivery	Supports DNS A, AAAA, A6, CNAME, DNAME, HINFO, KEY, MX, NS, NXT, PTR, SIG, SOA, SRV and TXR records	ADC should be a dedicated appliance, it should not work like a dedicated DNS server as it is already available in existing infra. **Suggested Clause:** **Appliance should be able to function as Authoritative Domain Name Server (ADNS), should be able to host AAAA Records, A Records and should also support DNSSEC**	Please be guided as per the RFP

		Controller (ADC) S. N. 540			
110.	RFP Page No. 35	Internet Router Specification	Atleast 2 Redundant AC/DC power supply	Request you to please clarify whether AC power or DC power supplies required	Please be guided as per the RFP
111.	RFP Page No. 35	Internet Router Specification	12x1/10GE WAN ports, 2X40GE and 2X40/100GE SPF/SPF+ base ports	Request to specify Exact Numbers and Type of SFPs required for terminating LAN & WAN Links and also please clarify its type (Copper/Multimode Fiber/Single Mode Fiber)	Please be guided as per the RFP
112.	RFP Page No. 36	Interconnect Switches Specification	24/48 nos. 25G/40G SFP/SFP+/QSFP based ports with 100G SFP/SFP+/QSFP+ based uplink Ports	kindly specify, whether 24 port switch or 48 port switch is required , also confirm number of 25G ports (1/10/25G ports) required and number of 40G ports required.	Please refer to the Corrigendum
113.	RFP Page No. 36	Interconnect Switches Specification	24/48 nos. 25G/40G SFP/SFP+/QSFP based ports with 100G SFP/SFP+/QSFP+ based uplink Ports	Request to specify exact Number of 100G SFP/SFP+/QSFP+ based uplink Ports	Please be guided as per the RFP
114.	RFP Page No. 70	DELIVERY & IMPLEMENTATION	Bidder shall be responsible for implementation (implementation team from respective OEM must be present onsite for the implementation) of the solution at both DC & DR or any other alternate site as per the Bank’s requirement.	Request to clarify if Professional Services from respective OEM to be considered for implementation	Please be guided as per the RFP
115.	RFP Page No.18	Supply, Implementation and Management of New devices - (f)	The entire data should be stored in masked/encrypted format and confirm to data privacy laws as prevailing during any time of the contract period	a) Kindly clarify which data needs to be masked or encryted , is there any data classification available b) Bidder understands that software/Infra required for data masking/encryption will be provided by Bank. Please confirm.	Please be guided as per the RFP
116.	RFP Page No.37	Miscellaneous	Bank is already contemplating implementation of next generation SOC with AI/ML capabilities. The Security Integrator is supposed to leverage the structured and unstructured data lying for event correlation and build analytics model based on AI/ML techniques & proactively warn the Bank of possible threats as per the Scope of work for SI services.	Please ammend this cluase as given below: "Bank is already contemplating implementation of next generation SOC with AI/ML capabilities. The Security Integrator is supposed to leverage the structured and unstructured data lying for event correlation and suggest SOC team to build analytics model based on AI/ML techniques &	Please be guided as per the RFP

				proactively warn the Bank of possible threats as per the Scope of work for SI services."	
117.	RFP Page No. 19	Components to be supplied by the bidder	Next Generation Firewall with application monitoring capability (Antivirus blade, SSL/ TLS decryptor, Application control, URL filtering licenses to cater Office 365 requirements, Anti-APT Internal scanning and sandboxing, Threat emulator/ NIPS) 14000 SSL VPN agent based remote VPN connection 200 site to site remote site VPN connection with at least 2TB of storage	1- Please confirm if Anti-APT and sandboxing are on premises 2- Please confirm if hash values or files can be shared to OEM cloud for zero day or unknown attacks	Please be guided as per the RFP
118.	RFP Page No. 28	Management of Existing Devices	Implement and maintain the security devices such as Check point firewall 23500(UTM), Forcepoint Webgate way/Proxy, Cisco Firepower 4200 firewall, Cisco Firepower 4250 NIPS, etc. appropriately as per the requirement which haven't reached their end of support	"Manage and maintain the security devices such as Check point firewall 23500(UTM), Forcepoint Webgate way/Proxy, Cisco Firepower 4200 firewall, Cisco Firepower 4250 NIPS, etc. appropriately as per the requirement which haven't reached their end of support" Please confirm if our understanding is correct	Please be guided as per the RFP
119.	RFP Page No. 37	Miscellaneous SOW	Security Integrator will liaise with OEM / Successful Bidder/ Vendor for the deployed devices for resolving problems as per Service Level Agreements.	To enable the bidder to maintain the desired uptime SLA of 99.90%, the bank must have back to back support/ATS/AMC from OEM of the existing inscope security solution. Please clarify.	Existing devices are under AMC/ATS/Support
120.	RFP Page No. 28	Onsite Technical Support-OTS	SI should liaison with the existing SI and vendors of the Bank and take handover of the architectural design, management and support of the components already deployed in the Bank from the existing vendor(s) within a period of 30 days from the deployment of onsite resources by the vendor	Kindly allow minimum three months for taking handover from existing agency.	Please be guided as per the RFP
121.	93	Limitation of Liability	***Clause 38(i) Any other breach caused due to the non-performance of the obligations of the Successful bidder under the Agreement***	Without deletion of this sub-clause, the liability capping to Contract Value has no significance and in effect it means Bank can claim damages, over the Total Contract Value , for breach of any of our obligations as vendor	Please be guided as per the RFP

122.	123	133. Other Features	Protection against DOS/DDOS attacks. Should have “self-learning" capability to monitor the network traffic and develops a baseline profile. It should have the ability to constantly update this profile to keep an updated view of the network.:- ■ Threshold and heuristic-based detection ■ Host-based connection limiting ■ Self-learning, profile-based detection	Clause stands deleted, corrigendum 1 (page 12, serial number 44)	Please be guided as per the RFP
123.	123	125. Other Features	Advanced DoS detection with "self-learning" for more accurate and fewer false positives.	This clause is dedicated DDOS appliance functionality and is also related to above clause which was deleted in corrigendum 1, but this got overlooked. We request you to kindly delete the same.	Please refer to the Corrigendum
124.	**141**	**Store minimum 15(Fifteen) days full Raw packets and 90(ninety) Days of indexed Meta data, having usable disk capacity of minimum 300 TB for raw packets & 100 TB for indexed metadata separately, after RAID configurations respectively having minimum 4 Ports (2 X 1Gbps Copper and 2X10 Gbps Fiber) on capture appliance. Bidder may factor additional storage as per the requirement**	**The average calculation for storing 20 Gbps of sustained traffic throughput over 24 hours for 15 days would be 3.164 Petabytes.** The average calculation for storing 20 Gbps of sustained traffic throughput over 24 hours for 15 days would be 3.164 Petabytes. If we assume bank working hours for sustained throughout is 12 hours (which is an ideal assumption), the storage required would still be 1.5 Petabytes. In the RFP, you have asked only 300 TB for raw packets which covers just 10- 12% of your retention requirements. Also, you are asked to factor additional storage as per requirements that means almost 90% of your retention requirements. Let us explain the storage calculations which is not any hidden formulae. You can also calculate it as explained below : **Storage required in TB** = ((((**Throughput in Gbps/8**)*3600) * **sustained throughput peak in hours**) * **no of days retention required**)/1024 **Legend:** **Throughput in Gbps** — Throughput required to be monitored by Bank	**In this context, we request you to ensure the retention storage size asked as per actual calculations to ensure bidders provide the minimum requirements required to achieve the retention period storage.** **Please help revise the storage requirements clause to actual requirements to help ensure bank does not end up in under supply or compromise on storage solution as SI’s bid will refer to listed numbers in RFP and commercial Bill of materials clauses.**	Please refer to the Corrigendum

<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td><b>8</b></td><td>No of bytes (conversion to size) to be generated</td></tr>
<tr><td><b>3600</b></td><td>Per hour size generated (60 seconds x 60 minutes)</td></tr>
<tr><td><b>Sustained throughout peak in hours</b></td><td>Assumption for no of peak sustained throughput hours – Based on work environment</td></tr>
<tr><td><b>1024</b></td><td>Convert total MB size in to TB</td></tr>
<tr><td colspan="2"><b>Example scenario</b>: For 12 hours sustained 20-Gbps peak throughput below is the formulae for storage calculation:</td></tr>
<tr><td colspan="2"><b>Storage required in TB</b> =((((20/8)*3600)*20)*15)/1024 which equals to 1582 TB</td></tr>
</table>
</td><td></td><td></td></tr>
<tr><td><b>125.</b></td><td colspan="4">Radware is a leading manufacturer for Application Delivery Controller & Cyber Security Solution and deployed various solution such as DDoS, IPS, WAF, Load Balancer, SSL Inspection in the existing infra of Punjab National Bank. The solution is running in existing infra from last many years to ensure availability and security. Despite being a LEADER in these technology, we are not able to participate (After latest corrigendum released) against above tender.</td><td>Please be guided as per the RFP</td></tr>
<tr><td><b>126.</b></td><td>Page 37 of 98</td><td>Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Anti DoS/ DDoS preventive module S. N. 33</td><td>Throughput:

Inspection and Mitigation: 20 Gbps
DDoS Flood Attack Prevention Rate: Minimum 30 Mpps
DDoS Cloud Mitigation: 4 Gbps</td><td>DDoS appliance is a transparent appliance and it should not be part of any stateful appliance. As per industry standard, DDoS sizing should be done based on inspection, mitigation and prevention rate. Appliance should have sufficient capacity to meet all the requirements. Mitigation throughput should always be doubled than Inspected throughput. Attack Prevention Rate should be inline with the throughpt asked, it should not be undersized.
DDoS appliance and Cloud should be from same OEM and both should be in sync including attack footprints to mitigate attack effectively. Cloud Scrubbing should be based out of India. It should not have any limitation in handling attack traffic and always ensure clean traffic of 4Gbps.

<b>Suggested Clause: Throughput:</b>

<b>Inspection Throughput: 30 Gbps</b></td><td>Please be guided as per the RFP</td></tr>
</table>

				Mitigation Throughput: 60 Gbps DDoS Flood Attack Prevention Rate: 40 Mpps **DDoS Cloud Mitigation: 4 Gbps legitimate Appliance and scrubbing from same OEM and both should be in sync including attack footprints. Scrubbing should be based in India and have capability to handle unlimited attacks**	
127.	Page 37 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Anti DoS/ DDoS preventive module S. N. 34	Throughput Scalability: Inspection and Mitigation: 40 Gbps (without additional hardware) Layer 4: 40 Gbps with 100 Million Hardware sync DDoS Flood Attack Prevention Rate: 35 Mpps without hardware change (This performance figure must be mentioned in public facing datasheet). DDoS Cloud Mitigation: 20 Gbps	DDoS appliance is a transparent appliance and it should not be part of any stateful appliance, it should have capability to detect and mitigate L3-7 attacks. There should not be any limitation on handling attack concurrent sessions. As per industry standard, DDoS sizing should be done based on inspection, mitigation and prevention rate. Solution should be sufficient scalable to handle all the requirements. **Suggested Clause: Throughput:** **Inspection Throughput: 60 Gbps** **Mitigation Throughput: 120 Gbps** **Attack Concurrent Sessions: Unlimited** **DDoS Flood Attack Prevention Rate: 100 Mpps without hardware change (This performance figure must be mentioned in public facing datasheet).** **DDoS Cloud Mitigation: 20 Gbps legitimate**	Please be guided as per the RFP
128.	Page 38 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Anti DoS/ DDoS	Ports: 8X 10G ports (SFP + Fiber port), 4x 40G (QSFP + Fiber port) ports 2 x 1G RJ45 Management Port . Fail to wire switch along with proposed device with minimum 4 bypass segment/ or can be achieved through additional external switch populated with same interfaces	Appliance should have sufficient port to cater current and future requirements. **Suggested Clause: Ports:** **12 X 10G ports (SFP + Fiber port),** **8 x 40G (QSFP + Fiber port) ports**	Please refer to the Corrigendum

		preventive module S. N. 37	capacity to achieve fail over or Achived through software by pass at interface level	**2 x 1G RJ45 Management Port and dedicated RJ45 Console Port** **Fail to wire switch along with proposed device with minimum 4 bypass segment/ or can be achieved through additional external switch populated with same interfaces** **capacity to achieve fail over or Achived through software by pass at interface level**	
129.	Page 38 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Anti DoS/ DDoS preventive module S. N. 40	Bidder has to provide threat intel solution from the OEMs of proposed systems for internal device consumption, in addition to the same bidder has to provide third party dedicated Threat Intelligence Feed from reputed OEMs. Third party Threat Intelligence Feed should able to provide analysis report/network graph analysis relation report based on historical data of the threat actor, threat activity, threat objects (historical data of the IPs, URLs, etc. used by the malicious entity, actors involved in the past incidences around the world), exploits run from the detected IPs, provide extensive context and malware analysis in addition to the threat indicators and any other valuable information. Search option should be available for minimum 5 analysts. Bidder has to factor necessary hardware/software/database etc for hosting above system in DC and DR if required. External threat intelligence system should be from renowned OEMs.	Leading OEM have their own threat intelligence feed to detect and mitigate TOR, Ruputation, IOC and Active Attackers based blocking and keep the system attacker free. **Suggested Clause:** **Bidder has to provide threat intel solution from the OEMs of proposed systems to detect and mitigate TOR, Ruputation, IOC and Active Attackers based blocking. Threat intelligence system should be from renowned OEMs.**	Please refer to the Corrigendum
130.	Page 38 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Anti DoS/ DDoS preventive module S. N. 41	The DDOS Appliance should support inbuilt Threat intelligence Gateway (TIG) feature for outbound threat blocking and should support third party threat feeds in industry standard STIX & TAXII format.	OEM should have its own threat intelligence feed to block mallicious threats. **Suggested Clause:** **The solution should support threat intelligence feed to block inbound/outbound threat**	Please refer to the Corrigendum
131.	Page 38 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component	Proposed product/solution should be stateless Technology not having any kind of state limitation e.g. TCP connections	As appliance asked is stateless in nature it should be able to handle unlimited attack concurrent sessions to avoid bottleneck in case of large attacks.It should not be part of any statefull appliance.	Please be guided as per the RFP

		Anti DoS/ DDoS preventive module S. N. 42		**Suggested Clause: Proposed product/solution should be stateless Technology not having any kind of state limitation e.g. TCP connections It should have capability to handle unlimited attack concurrent sessions.**	
132.	Page 39 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Anti DoS/ DDoS preventive module S. N. 48	a)Inbuilt mechanism to inspect traffic with external threat feed and shall support at least 3Million IOC's for inline blocking (URL, domain and IP address subnet) b)OPTIONAL: The solution has Inbuilt mechanism to inspect traffic with external threat intelligence feed and shall support at least 3Million hash for inline blocking	Leading OEM have their own threat intelligence feed to detect TOR, IP Ruputation, IOC blocking. **Suggested Clause:** **a)Inbuilt mechanism to inspect traffic with threat feeds (TOR, IP Reputation and IOC blocking)** **b)OPTIONAL: The solution has Inbuilt mechanism to inspect traffic with external threat intelligence feed and shall support at least 3Million hash for inline blocking**	Please refer to the Corrigendum
133.	Page 39 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Anti DoS/ DDoS preventive module S. N. 51	Support integration of external Threat Intelligence Platform (TIP) and Support Threat Intelligence Feed	Leading OEM have their own threat intelligence feed to detect mallicious threats in real time. **Suggested Clause: Support Threat Intelligence Feed**	Please refer to the Corrigendum
134.	Page 39 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Anti DoS/ DDoS preventive module S. N. 62	Support comprehensive countermeasure to protect against zero-day attack, Challenge - Response Mechanism, and which should be able to Detect and protect attacks in real time through inbuilt Captcha Mechanism or HTTP Authentication	Every OEM has its own method to detect and mitigate attacks, one method should not get higher marks verses other. Functionality should be supported. **Suggested Clause: Support comprehensive countermeasure to protect against zero-day attack, Challenge - Response Mechanism, and which should be able to Detect and protect attacks in real time through inbuilt Captcha Mechanism or HTTP Authentication or Equivalent.**	Please refer to the Corrigendum

				Equal marks for each method - Supports CAPTCHA- 5Marks (Max) Supports HTTP – 5Marks Supports(Equivalent)-5Marks	
135.	Page 40 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Anti DoS/ DDoS preventive module S. N. 71	Inspect SSL traffic for both RSA and ECC base key. Device should have support minimum 100,000 SSL TPS without session reuse for ECC & 2048 key RSA from day one and scalable up to 200,000 SSL TPS without hardware change	Appliance should not be oversized, it will unneccessary increase the overall cost. **Suggested Clause:** **Inspect SSL traffic for both RSA and ECC base key. Device should have support minimum 100,000 SSL TPS without session reuse for 2K key from day one and scalable up to 140,000 SSL TPS without hardware change.** **Key less functionality should also be supported.**	Please refer to the Corrigendum
136.	Page 42 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Anti DoS/ DDoS preventive module S. N. 104	Bandwidth should be dedicated and not shared. Connectivity required, if any, will have to be arranged and factored by the bidder.	OEM should ensure Clean bandwidth should be available always for the PNB. **Suggested Clause:** **OEM should provide scrubbing to mitigate unlimited attacks and ensure required legitimate throughput should always be available for PNB**	Please refer to the Corrigendum
137.	Page 43 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Network Intrusion Prevention System (NIPS) S. N. 111	Ports: Minimum of 4X10G copper ports with fail open and 6X40G QSFP+ fiber ports with fail open Dedicated 1 (1G / 100M) port for management console	As appliances has been asked in HA, fail-open is not required. Software fail-open can be considered like we have considered in DDoS. Sufficient SFP+ ports should be asked and it should not be copper port to cater current and future requirements. NIPS are transparent appliance, it should not be part of any statefull architecture and should not have any limitation on handling attack sessions. Only way to manage this appliance is through management port which should be redundant to avoid bottleneck in case of port failure, same has been considered for DDoS. Suggested Clause: **Ports:**	Please be guided as per the RFP

				Minimum of 12X10G SFP+ and 8X40G QSFP+ fiber ports with software bypass Dedicated 2 (1G / 100M) port for management and RJ45 for console **Appliance should be transparent and should not be part of any statefull appliance with unlimited attack concurrent session handling.**	
138.	Page 44 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Network Intrusion Prevention System (NIPS) S. N. 117	High availability in Active-active and active-passive mode with stateful failover and not only limited to transparent mode.	NIPS should always be transparent and stateless in nature to avoid bottleneck in case of attacks, appliance should not be visible to the attackers. **Suggested Clause: Support High availability with transparent and stateless in nature.**	Please be guided as per the RFP
139.	Page 44 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Network Intrusion Prevention System (NIPS) S. N. 132	Support Active-Active High Availability. It should support stateful HA such that state information is shared between the HA appliance. In case one of the appliances fails state is maintained. The HA should be out of the box solution and should not require any third party or additional software for the same	NIPS should always be transparent and stateless in nature, it can't host ip address on its interfaces. Hence, third pary is required for HA. **Suggested Clause: Support High Availability**	Please be guided as per the RFP
140.	Page 56 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Application Delivery Controller (ADC) with Threat Intelligence Gateway and SSL/TLS Offloader S. N. 264	CPU: 24 Physical Cores	12 Core CPU is sufficient to met the technical requirement, appliance should not be oversized. ADC appliance should be purpose built dedicated applliance. **Suggested Clause: CPU:** **12 Core**	Please be guided as per the RFP

141.	Page 56 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Application Delivery Controller (ADC) with Threat Intelligence Gateway and SSL/TLS Offloader S. N. 265	RAM: 256 GB	96GB RAM is sufficient to met the technical requirement, scalability should be considered. ADC appliance should be purpose built dedicated applliance. **Suggested Clause:** **RAM:** **96GB and scalable upto 192GB**	Please be guided as per the RFP
142.	Page 56 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Application Delivery Controller (ADC) with Threat Intelligence Gateway and SSL/TLS Offloader S. N. 267	Throughput: L7: 150 Gbps L7 requests:4.5M L4 requests:1.5M SSL TPS:100000 RSA 2048-bit keys SSL TPS: 90000 ECDSA P-256-bit	Appliance should not be oversized, it will unneccessary increase the overall cost. **Suggested Clause:** **Throughput:** **L4: 150 Gbps** **L7 requests:3M** **L4 requests:1.5M** **SSL TPS:60000 RSA 2048-bit keys** **SSL TPS: 30000 ECDSA P-256-bit**	Please be guided as per the RFP
143.	Page 56 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Application Delivery Controller (ADC) with Threat Intelligence Gateway and SSL/TLS Offloader S. N. 268	Throughput Scalability (without any additional hardware): L7: 175 Gbps L7 requests:6.5M L4 requests:2.5M SSL TPS: 200,000 RSA 2048-bit keys SSL TPS: 125,000 ECDSA P-256-bit	Appliance should not be oversized, it will unneccessary increase the overall cost. **Suggested Clause:** **Throughput:** **L4: 175 Gbps** **L7 requests:4M** **L4 requests:2.5M** **SSL TPS: 100,000 RSA 2048-bit keys** **SSL TPS: 45,000 ECDSA P-256-bit**	Please be guided as per the RFP
144.	Page 57 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Application Delivery Controller (ADC) with	SSL Offloading: 60 Gbps Scalable upto 90 Gbps (without any additional hardware)	Appliance should not be oversized, it will unneccessary increase the overall cost. **Suggested Clause:** **SSL Offloading:** **35 Gbps**	Please be guided as per the RFP

		Threat Intelligence Gateway and SSL/TLS Offloader S. N. 270		**Scalable upto 45 Gbps (without any additional hardware)**	
145.	Page 57 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Application Delivery Controller (ADC) with Threat Intelligence Gateway and SSL/TLS Offloader S. N. 271	Ports: 4*100G 16*25G	Appliance should not be oversized, it will unneccessary increase the overall cost. Management Port should be redundant to avoid port failure dependency. **Suggested Clause: Ports:** **2*100G** **16*25G** **Dedicated 2x1G RJ45 Management Port and RJ45 Console Port**	Please be guided as per the RFP
146.	Page 57 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Application Delivery Controller (ADC) with Threat Intelligence Gateway and SSL/TLS Offloader S. N. 272	Form Factor: 1RU (Preferably)	Hardware size should not restrict any OEM from Participation, 2RU should also be considered. **Suggested Clause:** **1RU/2RU (Preferably)**	Please refer to the Corrigendum
147.	Page 57 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Application Delivery Controller (ADC) with Threat Intelligence Gateway and SSL/TLS Offloader S. N. 273	Instances (Isolated): 20 scalable upto 35 (without any additional hardware)	Appliance should not be oversized, it will unneccessary increase the overall cost. **Suggested Clause:** **10 scalable upto 60 (without any additional hardware). Each instance should have dedicated Resource, Configuration, Management and Opertaing System.**	Please be guided as per the RFP

148.	Page 57 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Application Delivery Controller (ADC) with Threat Intelligence Gateway and SSL/TLS Offloader S. N. 274	The proposed solution as dedicated Hardware appliance based Next Generation Load Balancer, DNS, DNS Security and Global Server Load Balancing, Bot protection and API Security solution should be on single platform	There is a dedicated appliance has been asked to protect from DNS attacks, Bot and API protection. It should not be part of ADC. **Suggested Clause:** **The proposed solution as dedicated Hardware appliance based Next Generation Load Balancer, DNS and Global Server Load Balancing should be on single platform**	Please be guided as per the RFP
149.	Page 57 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Application Delivery Controller (ADC) with Threat Intelligence Gateway and SSL/TLS Offloader S. N. 275	The solution must support Reverse proxy or full proxy (Forward Proxy & Reverse Proxy) architecture for HTTP1.1 & HTTP/2 based application traffic. Support IPv6 for Reverse Proxy deployments, IPv4 to IPv6 and IPv6 to IPv4 Dual Stack communication. Device should have inbuilt SSL VPN capability for supporting users over VPN	There is a separate appliance has been asked to for VPN. It should not be part of ADC. **Suggested Clause:** **The solution must support Reverse proxy or full proxy (Forward Proxy & Reverse Proxy) architecture for HTTP1.1 & HTTP/2 based application traffic.** **Support IPv6 for Reverse Proxy deployments, IPv4 to IPv6 and IPv6 to IPv4 Dual Stack communication.**	Please be guided as per the RFP
150.	Page 57 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Application Delivery Controller (ADC) with Threat Intelligence Gateway and SSL/TLS Offloader S. N. 276	Always on management & LED to initial configuration	There should be dedicated redundant management port for management & reporting. Console Port should be used for intial configuration. LED should not be used for OEM restriction. **Suggested Clause:** **Always on management & console to initial configuration** **Dedicated 2x1G RJ45 Management Port and RJ45 Console Port**	Please refer to the Corrigendum
151.	Page 57 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Application Delivery	Capability to imply individual SSL certificate based on back-end application and remote end users secure communication. The solution should support Industry Standard Central Certificate Server integration feature so that new SSL certificate will be automatically update from central certificate server if existing certificate is expired.	ADC appliance should maintain required certificate and key to achieve SSL Offloading. **Suggested Clause:** **Capability to imply individual SSL certificate based on back-end application**	Please be guided as per the RFP

		Controller (ADC) with Threat Intelligence Gateway and SSL/TLS Offloader S. N. 281		**and remote end users secure communication. Should support Front end as well as Backend SSL.**	
152.	Page 59 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component SSL Inspection S. N. 301	CPU: 24 Physical Cores	12 Core CPU is sufficient to met the technical requirement, appliance should not be oversized. ADC appliance should be purpose built dedicated applliance. **Suggested Clause: CPU:** **12 Core**	Please be guided as per the RFP
153.	Page 59 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component SSL Inspection S. N. 302	Storage: Minimum 2x 1TB U.2 Enterprise-class SSD (RAID 1 Mirrored)	Log will be stored in smaller in size on an appliance whereas centralized management stores all the data required for reporting. Hence, 500GB SSD is sufficient for storage log on an appliance, same sizing has been cosidered for other components as well. **Suggsted Clause: Storage:** **Minimum 500GB SSD**	Please be guided as per the RFP
154.	Page 59 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component SSL Inspection S. N. 303	RAM: Minimum 256 GB	96GB RAM is sufficient to met the technical requirement, scalability should be considered. ADC appliance should be purpose built dedicated applliance. **Suggested Clause: RAM:** **96GB and scalable upto 192GB**	Please be guided as per the RFP
155.	Page 59 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component	Power on demand: Dual AC/DC supply with hot swappable units, with always on management & LED to initial configuration	There should be dedicated redundant management port for management & reporting. Console Port should be used for intial configuration. LED should not be used for OEM restriction.	Please refer to the Corrigendum

		SSL Inspection S. N. 304		**Suggested Clause:** **Dual AC/DC supply with hot swappable units, with always on management & console to initial configuration Dedicated 2x1G RJ45 Management Port and RJ45 Console Port**	
156.	Page 59 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component SSL Inspection S. N. 306	4*100G ports and 16*25G/10G with negotiable to 10G with SFP+/ QSFP+ as per the compatible interfaces	Appliance should not be oversized, it will unneccessary increase the overall cost. Management Port should be redundant to avoid port failure dependency. **Suggested Clause: Ports:** **2*100G ports and 16*25G/10G with negotiable to 10G with SFP+/ QSFP+ as per the compatible interfaces Dedicated 2x1G RJ45 Management Port and RJ45 Console Port**	Please be guided as per the RFP
157.	Page 60 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component SSL Inspection S. N. 309	Should support 200K SSL TPS of 2048 key size. Device should support both L2 and L3 deployment with ICAP support	Appliance should not be oversized, it will unneccessary increase the overall cost. ECC Cipher support should also be considered. **Suggested Clause: Should support 100K SSL TPS of 2048 key size and 45K SSL TPS of EC-P256. Device should support both L2 and L3 deployment. ICAP support should also be available on proposed solution.**	Please be guided as per the RFP
158.	Page 60 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component SSL Inspection S. N. 310	Device should provide ADC functionality as mentioned in RFP and should support virtualization.	The proposed device should support next generation features like Virtualization that can that virtualizes the Device resources—including CPU, memory, network, acceleration resources, Operating system to provide complete separate environment from applications and management perspective. Even if one virtual instance is rebooted it should not impact the other instances running on the same hardware.	Please be guided as per the RFP

				Suggested Clause : **Device should provide ADC functionality and should support next generation features like Virtualization that virtualizes the Device resources—including CPU, memory, network, operating system, and acceleration resources. Appliance should support virtualized as well as standalone mode.** **Each virtual ADC instance contains a complete and separated environment of the Following:** **a) Resources, b) Configurations, c) Management, d) Operating System** **Appliance should support 10vADC from day1 and scalable upto 50vADC.**	
159.	Page 60 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component SSL Inspection S. N. 311	L7 throughput of device should be minimum 180 Gbps	Appliance should not be oversized, it will unneccessary increase the overall cost. **Suggested Clause:** **L4 throughput of device should be minimum 180 Gbps**	Please be guided as per the RFP
160.	Page 60 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component SSL Inspection	New Clause Request	Filtering the traffic based on requirement should be part of SSL Inspection solution, it will ensure only the required traffic will be inspected and remaining will be bypassed. **Suggested Clause:** **Appliance should have URL filtering feature available**	Please be guided as per the RFP
161.	Page 60 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Web Application Firewall	CPU: 24 Physical Cores	12 Core CPU is sufficient to met the technical requirement, appliance should not be oversized. ADC appliance should be purpose built dedicated applliance. **Suggested Clause:** **CPU:**	Please be guided as per the RFP

		(WAF) S. N. 314		**12 Core**	
162.	Page 60 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Web Application Firewall (WAF) S. N. 315	RAM: 256 GB	96GB RAM is sufficient to met all the technical requirement, scalability should be considered. Appliance should not be oversized. **Suggested Clause: RAM:** **96 GB and scalable upto 192GB**	Please be guided as per the RFP
163.	Page 60 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Web Application Firewall (WAF) S. N. 321	Form Factor: 1RU (Preferably)	Hardware size should not restrict any OEM from Participation, 2RU should also be considered. **Suggested Clause:** **1RU/2RU (Preferably)**	Please refer to the Corrigendum
164.	Page 60 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Web Application Firewall (WAF) S. N. 322	Ports: 4*100G ports and 16*25G/10G with negotiable to 10G with SFP+/ QSFP+ as per the compatible interfaces	Appliance should not be oversized, it should have sufficient port to cater current and future requirements. Management port should be redundant to isolate port failure dependency. **Suggested Clause: Ports:** **2*100G ports and 16*25G/10G with negotiable to 10G with SFP+/ QSFP+ as per the compatible interfaces Dediacted 2x1G RJ45 Management Port and RJ45 Console Port**	Please be guided as per the RFP
165.	Page 63 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Web Application Firewall	a) Automatically update Certificate bundles from the appropriate CAs without any user intervention OR b) Appliance should maintain certificate and key repository	WAF should host certificate and key for an application to decrypt and inspect mallicius contect over secure channel https. Auto upadte of certifcate should not be part of WAF.	Please be guided as per the RFP

		(WAF) S. N. 360		**Suggested Clause. Appliance should maintain certificate and key repository**	
166.	Page 65 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Web Application Firewall (WAF) S. N. 377	The solution should provide online troubleshooting and traffic analysis tool where customer can take snapshot of appliance configuration and upload it on OEM's web based diagnostic tool to check the health and vulnerability of appliance with recommended solution provided on knowledge base link	Troubleshooting and analysis should be done offline with the help of TAC or onsite resource. OEM provides online site for knowledge and learning. **Suggested Clause:** **The solution should provide troubleshooting and traffic analysis. Proposed OEM should have dedicated online portal for knowledge and learning.**	Please be guided as per the RFP
167.	Page 67 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Web Application Firewall (WAF) S. N. 377	New Clause Request	Certification like ICSA, NSS and PCI-DSS is very important to choose right WAF solution, it will ensure right protection has been choosen to mitigate sophesticated attacks. **Suggested Clause:** **The WAF should be ICSA certified, NSS Lab Recommended and PCI Compliant**	Please be guided as per the RFP
168.	Page 67 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Web Application Firewall (WAF) S. N. 377	New Clause Request	The proposed device should support next generation features like Virtualization that can that virtualizes the Device resources—including CPU, memory, network, acceleration resources, Operating system to provide complete separate environment from applications and management perspective. Even if one virtual instance is rebooted it should not impact the other instances running on the same hardware. **Suggested Clause :** **The proposed Appliance should be dedicated hardware to support next generation features like Virtualization that virtualizes the Device resources—including CPU, memory, network, operating system, and acceleration**	Please be guided as per the RFP

				resources. **Each virtual ADC instance contains a complete and separated environment of the Following:** **a) Resources, b) Configurations, c) Management, d) Operating System Appliance should support 10vADC from day1 and scalable upto 50vADC.**	
169.	Page 67 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Web Application Firewall (WAF) S. N. 377	New Clause Request	WAF should have capability to send signal to DDoS to stop attacks at parameter itself, Attacker will not reach to WAF then. **Suggested Clause: Proposed WAF and DDoS Should integrate with each other. It should have a unique Messaging mechanism that efficiently mitigates attacks by sending attack information to DDoS located at the Network Perimeter.**	Please be guided as per the RFP
170.	Page 76 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Network Load Balancer(NLB), Global Site Load Balancer(GSLB) external Application Delivery Controller (ADC) S. N. 498	CPU: 24 Core	12 Core CPU is sufficient to met all the technical requirement, appliance should not be oversized. ADC appliance should be purpose built dedicated appliance. **Suggested Clause: CPU:** **12 Core**	Please be guided as per the RFP
171.	Page 76 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Network Load Balancer(NLB), Global Site Load Balancer(GSLB) external	RAM: 256GB	96GB RAM is sufficient to met the technical requirement, scalability should be considered. **Suggested Clause: RAM:** **96 GB and scalable upto 192GB**	Please be guided as per the RFP

		Application Delivery Controller (ADC) S. N. 500			
172.	Page 76 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Network Load Balancer(NLB), Global Site Load Balancer(GSLB) external Application Delivery Controller (ADC) S. N. 505	Ports: (4X40GE QSFP+ SR4 or 4X100GE SFP+ Ports) and (8X10GE SFP+ ports) SFP+/QSFP+ 1X1G Management port All ports should be fully populated	Appliance should not be oversized, it will unneccessary increase the overall cost without any specific requirement. Management Port should be redundant to avoid port failure dependency. **Suggested Clause: Ports:** **(4X40GE QSFP+ SR4 or 2X100GE SFP+ Ports)** **and** **(8X10GE SFP+ ports) SFP+/QSFP+** **Dedicated 2x1G RJ45 Management Port and RJ45 Console Port** **All ports should be fully populated**	Please be guided as per the RFP
173.	Page 76 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Network Load Balancer(NLB), Global Site Load Balancer(GSLB) external Application Delivery Controller (ADC) S. N. 507	Virtual Instances 15, scalable to 20 with complete network & resource isolation	Appliance should not be oversized, it will unneccessary increase the overall cost. **Suggested Clause:** **10 scalable upto 50 (without any additional hardware). Each instance should have dedicated Resource, Configuration, Management and Opertaing System.**	Please be guided as per the RFP
174.	Page 77 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Network Load Balancer(NLB), Global Site Load Balancer(GSLB) external	The ADC shall be manageable by SSH , HTTP, HTTPS, API, Console	Secure channel should be used for authentication. **Suggested Clause:** **The ADC shall be manageable by SSH , HTTPS, API, Console**	Please refer to the Corrigendum

		Application Delivery Controller (ADC) S. N. 518			
175.	Page 77 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Network Load Balancer(NLB), Global Site Load Balancer(GSLB) external Application Delivery Controller (ADC) S. N. 522	The proposed solution as dedicated Hardware appliance based Next Generation Load Balancer, DNS, DNS Security and Global Server Load Balancing, should be on single platform	There is a dedicated hardware DDOS has been asked to protect DNS attacks. Asking the same features again on ADC without any spcific requirement will unneccessary increase the overall cost. **Suggested Clause:** **The proposed solution as dedicated Hardware appliance based Next Generation Load Balancer, DNS and Global Server Load Balancing, should be on single platform**	Please be guided as per the RFP
176.	Page 77 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Network Load Balancer(NLB), Global Site Load Balancer(GSLB) external Application Delivery Controller (ADC) S. N. 523	The solution must support Reverse proxy or full proxy (Forward Proxy & Reverse Proxy) architecture for HTTP1.1 & HTTP/2 based application traffic. Support IPv6 for Reverse Proxy deployments, IPv4 to IPv6 and IPv6 to IPv4 Dual Stack communication. Device should have inbuilt SSL VPN capability.	There is a dedicated solution for authentication/VPN has been asked in the RFP. Asking the same features again on ADC without any spcific requirement will unneccessary increase the overall cost. **Suggested Clause:** **The solution must support Reverse proxy or full proxy (Forward Proxy & Reverse Proxy) architecture for HTTP1.1 & HTTP/2 based application traffic. Support IPv6 for Reverse Proxy deployments, IPv4 to IPv6 and IPv6 to IPv4 Dual Stack communication**	Please be guided as per the RFP
177.	Page 78 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Network Load Balancer(NLB), Global Site Load Balancer(GSLB) external Application Delivery	The solution must have ICAP integration with other security devices for file vulnerability, virus, Trojan scanning during file submission with webapplications to improve security or equivalent or built-in AV	ICAP integration can't be part of ADC with LB, it will unneccessary increase the overall cost without any specific requirement. **Suggested Clause:** **Delete the clause**	Please be guided as per the RFP

		Controller (ADC) S. N. 528			
178.	Page 79 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Network Load Balancer(NLB), Global Site Load Balancer(GSLB) external Application Delivery Controller (ADC) S. N. 540	Supports DNS A, AAAA, A6, CNAME, DNAME, HINFO, KEY, MX, NS, NXT, PTR, SIG, SOA, SRV and TXR records	ADC should be a dedicated appliance, it should not work like a dedicated DNS server as it is already available in existing infra. **Suggested Clause: Appliance should be able to function as Authoritative Domain Name Server (ADNS), should be able to host AAAA Records, A Records and should also support DNSSEC**	Please be guided as per the RFP
179.	Page 37 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Anti DoS/ DDoS preventive module S. N. 33	Throughput: Inspection and Mitigation: 20 Gbps DDoS Flood Attack Prevention Rate: Minimum 30 Mpps DDoS Cloud Mitigation: 4 Gbps	DDoS appliance is a transparent appliance and it should not be part of any stateful appliance. As per industry standard, DDoS sizing should be done based on inspection, mitigation and prevention rate. Appliance should have sufficient capacity to meet all the requirements. Mitigation throughput should always be doubled than Inspected throughput. Attack Prevention Rate should be inline with the throughpt asked, it should not be undersized. DDoS appliance and Cloud should be from same OEM and both should be in sync including attack footprints to mitigate attack effectively. Cloud Scrubbing should be based out of India. It should not have any limitation in handling attack traffic and always ensure clean traffic of 4Gbps. **Suggested Clause: Throughput:** **Inspection Throughput: 30 Gbps** **Mitigation Throughput: 60 Gbps** **DDoS Flood Attack Prevention Rate: 40 Mpps**	Please be guided as per the RFP

				DDoS Cloud Mitigation: 4 Gbps legitimate Appliance and scrubbing from same OEM and both should be in sync including attack footprints. Scrubbing should be based in India and have capability to handle unlimited attacks	
180.	Page 37 of 98	Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component Anti DoS/ DDoS preventive module S. N. 33	Throughput: Inspection and Mitigation: 20 Gbps DDoS Flood Attack Prevention Rate: Minimum 30 Mpps DDoS Cloud Mitigation: 4 Gbps	DDoS appliance is a transparent appliance and it should not be part of any stateful appliance. As per industry standard, DDoS sizing should be done based on inspection, mitigation and prevention rate. Appliance should have sufficient capacity to meet all the requirements. Mitigation throughput should always be doubled than Inspected throughput. Attack Prevention Rate should be inline with the throughpt asked, it should not be undersized. DDoS appliance and Cloud should be from same OEM and both should be in sync including attack footprints to mitigate attack effectively. Cloud Scrubbing should be based out of India. It should not have any limitation in handling attack traffic and always ensure clean traffic of 4Gbps. **Suggested Clause: Throughput:** **Inspection Throughput: 30 Gbps** **Mitigation Throughput: 60 Gbps** **DDoS Flood Attack Prevention Rate: 40 Mpps** **DDoS Cloud Mitigation: 4 Gbps legitimate Appliance and scrubbing from same OEM and both should be in sync including attack footprints. Scrubbing should be based in India and have capability to handle unlimited attacks**	Please be guided as per the RFP

181.	3	Storage	Minimum 400 GB SSD for system and 2 TB SSD for Logging capability	No other OEM other then Palo Alto do support such storage requirement of 400GB SSD for system and its been copy pasted from the datasheet of Palo Alto. Atleast give fair chance to Fortinet to participate, else this is proprietary purchase. Kindly update it as: "Minimum 400 GB SSD for system and 2TB SSD for logging capability" . It is specific to PA-5450 Chassis. Please refer to storage capacity on page 6 in the datasheet.	Please refer to the Corrigendum.
182.	4	Throughput	Inspection throughput- 30 Gbps IPsec VPN - 15 Gbps(AES256-SHA256) New Sessions-615,000 per second Concurrent Sessions -20M	Again to give undue advantage to Palo Alto, new sessions not been increased and been kept 615K where as in scalability its been increased. So that Palo Alto can give complete solution with 2 solution and Fortinet has to give 6 blades. As per standard concurrent session : new session to be 10:1. So New sessions has to 2 million atleast or 1 million. Kindly update clause as: Inspection throughput- 30 Gbps IPsec VPN - 15 Gbps(AES256-SHA256) New Sessions-615,000 per second 1.0 Million per second Concurrent Sessions -20M.	Please be guided as per the RFP
183.	5	Throughput Scalability	Inspection throughput- 120 Gbps IPsec VPN - 30 Gbps(AES256-SHA256) New Sessions- 3.2 Million per second Concurrent Sessions -50Million	The way specs has been changed after corrigendum is to make qualify lower model of Palo Alto-5450 and Fortinet to position FG-7121F with 6 blades. This makes price difference of 6 times and making Fortinet to not get fair chance to participate commecially. PA model 5450 has maximum 3.6 million session and its been asked 3.2 million. Where as per standard ration between concurrent session : new session is 1:10; accordingly this has to be 5 million. But to give undue advantage to Palo Alto (single OEM) 3.2 million has been kept so	Please be guided as per the RFP

				that no other OEM able to beat Palo Alto commercially. Attaching snapshot of appliance. Initially it was 100 Gbps t0 make Fortinet commercially unviable, it is been increased from 100 Gbps to 120 Gbps. Kindly make change as follows: Inspection throughput- 120 Gbps 100 Gbps IPsec VPN - 30 Gbps(AES256-SHA256) New Sessions- 3.2 Million per second 3.0 Million per second Concurrent Sessions -50Million. It is specific to PA-5450 Chassis. Please refer to Performance and capacity on page 5 in the datasheet.	
184.	9	Ports	12X10 Gig SFP/SFP+ ports with respective SR transceivers & 2 x 40G/100G QSFP28 ports with respective transceivers Console Management USB Port 4 X 1/10 Gig Ethernet	Initially port requirement were much more and suddenly after corrigendum it is decreased to give undue advantage to Palo Alto in pricing and making other competitor to position biggest appliance with fully populated configuration. Kindly change the port quantity so that we have fair chance to participate. 12X10 Gig SFP/SFP+ ports with respective SR transceivers & 2 x 40G/100G QSFP28 ports with respective transceivers Console Management USB Port 4 X 1/10 Gig Ethernet 2 X 1 Gig Ethernet (else fortinet will be dis qualified in any of the models). It is specific to PA-5450 Chassis. Please refer to Hardware Specifications on page 6 in the datasheet	Please refer to the Corrigendum.
185.	13	Form Factor	Maximum 5U(Preferably) in standard 42U Rack	The way all specification been sesigned, immidiately after the corrigendum been changed to qualify only Palo Alto. Fortinet to give 42U appliance and PA can give in 5U. As per specs on 5U is to be qualified. This is made specifically to Palo Alto, so that	Please refer to the Corrigendum.

				no other OEM do participate. Size shouldnt be defined and kept open as per solution. Attaching snap shot of Palo Alto from where specs been made and copy paste. "Point to be deleted". It is specific to PA-5450 Chassis. Please refer to Rack Mount (Dimensions) on page 6 in the datasheet	
186.	23		Dashboard view and reporting of CPU usage (including realtime graph) for management activities and data plane CPU for other activities.	This is specific to Palo Alto, please make the below change to make Fortinet qualify: Dashboard view and realtime graph of CPU, Memory,Session usage activity. And should the option to view the CPU and memory usages for management activities and data plane CPU for other activities.. PA Feature Please refer to link - https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PLKKCA4	Please refer to the Corrigendum.
187.	24		Minimum NG Threat prevention throughput in real world/production/Application Mix environment (by enabling and measured with Application-ID, AVC, NGIPS, Anti-Virus, Anti-Malware, Anti-Spyware and logging enabled should be 30 Gbps. The bidder shall submit the performance test report reference from public documents or from Global Product Engineering department / Global Testing Department/ Global POC team of OEM certifying the mentioned performance and signed by person with PoA. Optional : The device may also have support for zero day attack prevention and file blocking security threat prevention features	This is specific to Palo Alto, please make the below change to make Fortinet qualify: Minimum NG Threat prevention throughput in real world/production/Application Mix environment (by enabling and measured with Application-ID/AVC, NGIPS, Anti-Virus/ Anti-Malware/ Anti-Spyware and logging enabled should be 30 Gbps. The bidder shall submit the performance test report reference from public documents or from Global Product Engineering department / Global Testing Department/ Global POC team of OEM certifying the mentioned performance and signed by person with PoA. Optional : The device may also have support for zero day attack prevention and file blocking security threat prevention features. It is specific to PA-5450 Chassis. Please refer to Threat Prevention throughput on page 5 in the datasheet.	Please refer to the Corrigendum

				Testing Blades - Threat Prevention throughput is measured with App-ID, IPS, antivirus, antispyware, WildFire, DNS Security, file blocking, and logging enabled, utilizing 64 KB HTTP/appmix transactions	
188.	25		Support for both Client as well client less VPN. Must support Split tunneling based on destination domain, client process, and video streaming application. Solution must support App for endpoints running Windows, Linux and macOS and also should support Mobile app for endpoints running iOS, Android, Chrome OS, and Windows 10.	This is specific to Palo Alto, please make the below change to make Fortinet qualify: Support for both Client as well client less VPN. Must support Split tunneling based on destination domain, client process, and video streaming application. Solution must support App for endpoints running Windows, Linux and macOS and also should support Mobile app for endpoints running iOS, Android, Chrome OS, and Windows 10.. It is specific to PA global protect client. Please refer to GlobalProtect App Supported Platforms on page 6 in the datasheet.	Please refer to the Corrigendum
189.	33		GUI based packet capture utility within its management console with capability of creating packet capture filters for IPv4 and IPv6 traffic and ability to define the packet and byte count	Every OEM has their own way to provide feature and functionality. Fortinet can also propose some functionlaity which makes Palo Alto to be dis qualified. Here in complete RFP all points pertainging to Palo been captures so that Fortinet doesnt qualify.Kindly make below change for us to quaify. GUI based packet capture utility within its management console with capability of creating packet capture filters for IPv4 and IPv6 traffic and ability to define the packet and or byte count. Palo Alto OS feature. Refer to following link - https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/monitoring/take-packet-captures/take-a-custom-packet-capture#id612bf3c8-c075-44a0-b120-aca11fd2abd3	Please refer to the Corrigendum.

190.	57		Should have Host inspection profiling and it should collect information about the host it is running on. The VPN client should submit host information to the gateway upon successful connection. The gateway should match this information with HIP profiles on the NGFW and accordingly NGFW should enforce the corresponding security policy.	This is specific to Palo Alto, please make the below change to make Fortinet qualify: Should have Host inspection profiling and it should collect information about the host it is running on. The VPN client should submit host information to the gateway/Client management server upon successful connection. The gateway should match this information with HIP profiles on the NGFW or Client Management server and accordingly NGFW should enforce the corresponding security policy.. It is specific to PA feature . Refer to link - https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/globalprotect/objects-globalprotect-hip-profiles	Please refer to the Corrigendum.
191.	61		The NGFW should have native protection against credential theft attacks (without the need of endpoint agents) with ability to prevent the theft and abuse of stolen credentials and the following : · Automatically identify and block phishing sites · Prevent users from submitting credentials to phishing sites · Prevent the use of stolen credential	This is specific to Palo Alto, please make the below change to make Fortinet qualify: The NGFW should have native protection against credential theft attacks (without the need of endpoint agents) with ability to prevent the theft and abuse of stolen credentials and the following : · Automatically identify and block phishing sites · Prevent users from submitting credentials to phishing sites · Prevent the use of stolen credential. It is part of PA feature. Refer to link - https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/threat-prevention/prevent-credential-phishing	Please refer to the Corrigendum.
192.	80		OPTIONAL: The solution can use AV and zero day signatures based on payload and not just by hash values and it can support bare metal analysis if required. The advanced malware analysis	This is specific to Palo Alto, please make the below change to make Fortinet qualify: OPTIONAL: The solution can use AV and	Please refer to the Corrigendum.

<table>
<tr><td></td><td></td><td></td><td>(malware sandboxing) solution must have MacOS and Linux executable scanning by default.</td><td>zero day signatures based on payload and not just by hash values and it can support bare metal analysis if required. The advanced malware analysis (malware sandboxing) solution must have MacOS and Linux executable scanning by default.. It is specific to PA. Please refer to link - https://docs.paloaltonetworks.com/wildfire/9-1/wildfire-admin/wildfire-overview/wildfire-concepts/analysis-environment</td><td></td></tr>
<tr><td><b>193.</b></td><td>120</td><td></td><td>Acquire User Identities from: LDAP, Captive Portal, VPN, NACs (XML or API), Syslog, Terminal Services, XFF Headers, Server Monitoring, AND client probing</td><td>This is specific to Palo Alto, please make the below change to make Fortinet qualify:

Acquire User Identities from: LDAP, Captive Portal, VPN, NACs (XML or API), Syslog, Terminal Services, XFF Headers, Server Monitoring, AND client probing. It is part of PA feature. Please refer to link -

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/user-id/enable-user-id</td><td>Please refer to the Corrigendum.</td></tr>
<tr><td><b>194.</b></td><td><b>71</b></td><td><b>8. Payment terms</b></td><td><table><tr><td><b>8. Payment Terms</b></td><td rowspan="2"><b>Deliverables</b></td><td rowspan="2"><b>Timelines</b></td><td rowspan="2"><b>Payment Terms</b></td><td rowspan="2"><b>Payment Amount</b></td></tr><tr><td>(A – Device Cost</td></tr></table></td><td><table><tr><td><b>Deliverables</b></td><td><b>Timelines</b></td><td><b>Payment Terms</b></td><td><b>Payment Amount</b></td></tr></table></td><td>Please be guided as per the RFP</td></tr>
</table>

				B – Implementation Cost	Delivery of all the Devices and applicable Licenses, wherever applicable after release of P.O.	Within 12 weeks from date of Purchase Order (P.O.)	After submission of PBG, delivery of hardware, licenses and deployment of OTS Resources	50 % of A		Delivery of all the Devices and applicable Licenses, wherever applicable after release of P.O.	Within 18 weeks from date of PO	After delivery of hardware and licenses.	**70 %** of A	
				C – AMC Cost				50% of E					**70 %** of E	
				D – ATS Cost	Installation & Integration of all the Devices & Go-live of entire solution, Sign off,	Within 20 weeks from the date of P.O	After sign-off post successful implementation	50% of A		Installation & Integration of all the Devices & Go-live of entire solution, Sign off,	Within 32 weeks from delivery date*	After sign-off post successful implementation	**30%** of A	
				E – License Cost				50% of B					**70%** of B	
				F – FM Services/ OTS)				50% of E					**30%** of E	
						After 90 days from signoff	90 days after sign-off	50% of B			After 90 days from signoff	90 days after sign-off	**30%** of B	

<table>
<tr>
<td></td>
<td></td>
<td></td>
<td><table><tr><td></td><td>AMC/ATS# Cost of Devices/Solution/Components</td><td>N/A</td><td>To be raised at the start of each quarter</td><td>Quarterly in Advance basis on production of requisite documents**</td></tr><tr><td></td><td>OTS Cost</td><td>N/A</td><td>To be raised after end of each quarter</td><td>Quarterly on arrear basis</td></tr></table></td>
<td><table><tr><td>AMC/ATS# Cost of Devices/Solution/Components</td><td>N/A</td><td>To be raised at <b>the beginning of each year</b></td><td><b>Yearly</b> in Advance basis on production of requisite documents**</td></tr><tr><td>OTS Cost</td><td>N/A</td><td>To be raised at <b>the beginning of each</b> quarter</td><td>Quarterly on <b>Advance</b> basis</td></tr></table></td>
<td></td>
</tr>
<tr>
<td><b>195.</b></td>
<td>139</td>
<td>444</td>
<td>Analysis engine must support micro-tasking within Dynamic Analysis O.S VM's (Windows, Macintosh & Linux environments), such as analysis using different versions and service packs of operating systems and different versions of applications by performing the analysis in parallel (i.e. To use multiple virtual machines in parallel) with all licenses and dependencies included in the platform.</td>
<td>Request to remove Mac OS or make it optional. Analysis engine must support micro-tasking within Dynamic Analysis O.S VM's (Windows, Macintosh/Linux environments), such as analysis using different versions and service packs of operating systems and different versions of applications by performing the analysis in parallel (i.e. To use multiple virtual machines in parallel) with all licenses and dependencies
included in the platform.
Request to remove Mac OS or make it optional</td>
<td>Please refer to the Corrigendum</td>
</tr>
<tr>
<td><b>196.</b></td>
<td>Corrigendum Page 72</td>
<td>462.</td>
<td>Solution must have a dedicated <b>on premises</b> Malware Analysis engine with purpose built platform having windows, Linux and MAC O.S environments. <b>Bidder may size the system as per the best available option.</b></td>
<td>Request to remove Mac OS or make it optional. Solution must have a dedicated on premises Malware Analysis engine with purpose built platform having windows, Linux / MAC O.S environments. Bidder may size the system as per the best available option.
Request to remove Mac OS or make it optional</td>
<td>Please refer to the Corrigendum</td>
</tr>
</table>

197.		492.	Store minimum **15(Fifteen)** days full Raw packets and 90(ninety) Days of indexed Meta data, having usable disk capacity of minimum 300 TB for raw packets & 100 TB for indexed metadata separately, after RAID configurations respectively having minimum 4 Ports (2 X 1Gbps Copper and 2X10 Gbps Fiber) on capture appliance. **Bidder may factor additional storage as per the requirement**	It is mathematically impossible to keep 20G raw traffic for 15 days on 300 Tb storage. This will require =20000000000/(8*1024*1024*1024)*3600*24*15 = 3017 Tb. So it requires 10 times more space. And for 7 days the storage space for 20Gbps will be ~1600Tb. Request you to increase the storage size accordingly.. Store minimum 07(Seven) days full Raw packets and 90(ninety) Days of indexed Meta data, having usable disk capacity of minimum 300 TB for raw packets & 100 TB for indexed metadata separately, after RAID configurations respectively having minimum 4 Ports (2 X 1Gbps Copper and 2X10 Gbps Fiber) on capture appliance. Bidder may factor additional storage as per the requirement	Please refer to the Corrigendum
198.		497.	Solution should Include O.S environment support for Windows, Linux and MacOS X systems, completely on-premise. No Submissions should require to be submitted on cloud or 3rd party. All requirements, updates, upgrades, patches must be provided for the solution by the bidder to run for entire project period	Request to remove Mac OS or make it optional. Solution should Include O.S environment support for Windows, Linux /MacOS X systems, completely on-premise. No Submissions should require to be submitted on cloud or 3rd party. All requirements, updates, upgrades, patches must be provided for the solution by the bidder to run for entire project period	Please refer to the Corrigendum
199.		Corrigendum 1 - RFP for Procurement and Management of Cyber Security Component.pdf Clause number 149	Throughput scalability Clause number 149 page number 46 in published Corrigendum 1 is not revised/updated as per the response (Response published - Sl No.52 page number 13 in Corrigendum 1) Existing Clause: Original Tender *Inspection throughput- 100 Gbps* *IPsec VPN - 30 Gbps(AES256-SHA256)* *Sessions- 1,000,000 per second* *Concurrent Sessions -50M* As clarified in corrigendum 1: Refer Sl No.52 page number 13 Inspection throughput- 120 Gbps	As clarified in corrigendum 1: Refer Sl No.52 page number 13 Inspection throughput- 120 Gbps IPsec VPN - 30 Gbps(AES256-SHA256) New Sessions- 3.2 Million per second Concurrent Sessions -50 Million Revised clause still refers the pre-corrigendum numbers and thus creating a ambiguity on the throughput ask.Seeking clarification to propose the solution which	Please refer to the Corrigendum

			IPsec VPN - 30 Gbps(AES256-SHA256) *New Sessions- 3.2 Million per second* *Concurrent Sessions -50 Million* New Clause as per ANNEXURE-XI(A) in corrigendum 1: Refer clause number 149 page number 46 *Inspection throughput- 100 Gbps* *IPsec VPN - 30 Gbps(AES256-SHA256)* *Sessions- 1,000,000 per second* *Concurrent Sessions -50M* Revised clause still refers the pre-corrigendum numbers and thus creating a ambiguity on the throughput ask.Seeking clarification to propose the solution which adheres to the PNB ask and able to meet the scalabilty in future.	adheres to the PNB ask and able to meet the scalabilty in future.	
200.		Corrigendum 1 - RFP for Procurement and Management of Cyber Security Component.pdf Clause number 148	As per the RFP ask PNB Bank is looking for an upgrade to Next Generation Firewall .Please clarify if the inspection throughput asked in the clause number 148,149 on page number 46 in corrigendum 1 is NGFW throghput .We request Bank to please clarify to ensure that the proposed device meets the solution requirement.	As per the RFP ask PNB Bank is looking for an upgrade to Next Generation Firewall .Please clarify if the inspection throughput asked in the clause number 148,149 on page number 46 in corrigendum 1 is NGFW throghput .We request Bank to please clarify to ensure that the proposed device meets the solution requirement.	Please refer to the Corrigendum
201.		**23**	8X 10G ports (SFP + Fiber port), 4x 40G (QSFP + Fiber port) ports 2 x 1G RJ45 Management Port . Fail to wire switch along with proposed device with minimum 4 bypass segment/ or can be achieved through additional external switch populated with same interfaces capacity to achieve fail over or Achived through software by pass at interface level	8X 10G ports (SFP + Fiber port), 2x 40G (QSFP + Fiber port) ports 2 x 1G RJ45 Management Port . Fail to wire switch along with proposed device with minimum 4 bypass segment/ or can be achieved through additional external switch populated with same interfaces capacity to achieve fail over or Achieved through software by pass at interface level	Please refer to the Corrigendum
202.		71	Inspect SSL traffic for both RSA and ECC base key. Device should have support minimum 100,000 SSL TPS without session reuse for ECC & 2048 key RSA from day one and scalable up to 200,000 SSL TP S without hardware change	Request to remove this point as its specific to Application Delivery Controller and Load Balancer. As far as Anti-DDoS is concerned, SSL CPS specification is covered in original RFP Page 121 point # 63 and Corrigendum Page 40 point # 65	Please refer to the Corrigendum

203.		34	OEM shall provide scrubbing to mitigate unlimited number of attacks and has to ensure that the required legitimate throughput should always be available for the Bank.	Bidder/MSSP/ISP/OEM shall provide scrubbing services to mitigate unlimited number of attacks and has to ensure that the required legitimate throughput should always be available for the Bank.	Please refer to the Corrigendum
204.		106	Service should be always on	Service should be always on or On-Demand Protection	Please refer to the Corrigendum
205.		466	Store minimum 15(Fifteen) days full Raw packets and 90(ninety) Days of indexed Meta data, having usable disk capacity of minimum 300 TB for raw packets & 100 TB for indexed metadata separately, after RAID configurations respectively having minimum 4 Ports (2 X 1Gbps Copper and 2X10 Gbps Fiber) on capture appliance. Bidder may factor additional storage as per the requirement	The average calculation for storing 20 Gbps of sustained traffic throughput over 24 hours for 15 days would be 3.164 Petabytes. If we assume bank working hours for sustained throughout is 12 hours (which is an ideal assumption), the storage required would still be 1.5 Petabytes. In the RFP, you have asked only 300 TB for raw packets which covers just 10- 12% of your retention requirements. Also, you are asked to factor additional storage as per requirements that means almost 90% of your retention requirements. Let us explain the storage calculations which is not any hidden formulae. You can also calculate it as explained below : Storage required in TB = ((((Throughput in Gbps/8)*3600) * sustained throughput peak in hours) * no of days retention required)/1024 Legend: Throughput in Gbps Throughput required to be monitored by Bank 8 No of bytes (conversion to size) to be generated 3600 Per hour size generated (60 seconds x 60 minutes) Sustained throughout peak in hours Assumption for no of peak sustained throughput hours – Based on work	

				environment 1024 Convert total MB size in to TB Example scenario: For 12 hours sustained 20-Gbps peak throughput below is the formulae for storage calculation: Storage required in TB =((((20/8)*3600)*20)*15)/1024 which equals to 1582 TB. In this context, we request you to ensure the retention storage size asked as per actual calculations to ensure bidders provide the minimum requirements required to achieve the retention period storage. Please help revise the storage requirements clause to actual requirements to help ensure bank does not end up in under supply or compromise on storage solution as SI's bid will refer to listed numbers in RFP and commercial Bill of materials clauses.	
206.			OEM shall provide scrubbing to mitigate unlimited number of attacks and has to ensure that the required legitimate throughput should always be available for the Bank.	Bidder shall provide scrubbing services to mitigate unlimited number of attacks and has to ensure that the required legitimate throughput should always be available for the Bank.	Please refer to the Corrigendum
207.	**INSPIRA ENTERPIRSE**	Shift Planning of Resources	Resource List	Kindly confirm the number of L1 resources (36 at DC & 3 at DRC) to be deployed at DC and RDC in each shift. As per our understanding 12 L1 engineer to be deployed in each shif t i.e. Morning Shift, Afternoon Shift and Night Shift. Kindly confirm.	Please be guided as per the RFP
208.	**INSPIRA ENTERPIRSE**	SCORING METHODOLOGY	Marks on resources experience – As per the manpower skillset mentioned in the RFP, only L4 and L3 resources are asked to be CCIE/CISSP certified. And the total requirement of L4 and L3 resouces are 1 and 2 respectively. 1. 1 marks for minimum 10 CCIE/CISSP in the organisation for experience of minimum 5 years. But in Scoring Methodology	As per the manpower skillset mentioned in the RFP, only L4 and L3 resources are asked to be CCIE/CISSP certified. And the total requirement of L4 and L3 resouces are 1 and 2 respectively.	Please be guided as per the RFP

			you have asked that bidders should have at least 10 CCIE/CISSP certified reosurces to obtain 1 marks. And in order to obtain a maximum marks of 5 bidder has to submit the details of at least 50 CCIE/CISSP certified resources. 2. 0.5 mark per CCIE/CISSP certified resource above 10 resources having experience of more than 5 years (Undertaking along with duly Bio Data of onsite resource experience to be submitted. Employee should be on company payroll) We request you to kindly relax and amend this clause as: 5 marks for minimum 5 CCIE/CISSP in the organisation for experience of minimum 5 years.	But in Scoring Methodology you have asked that bidders should have at least 10 CCIE/CISSP certified reosurces to obtain 1 marks. And in order to obtain a maximum marks of 5 bidder has to submit the details of at least 50 CCIE/CISSP certified resources. We request you to kindly relax and amend this clause as: 5 marks for minimum 5 CCIE/CISSP in the organisation for experience of minimum 5 years.	
209.	**HITACHI**	Sir as you are aware that shortages of Router and switches in globally include, but are not limited to: chips, memory, mechanical raw materials, power supplies and fans, which have resulted in cost increases, longer lead delivery times i.e more than one year . We therefore request to kindly amend the delivery timeline for Router & Switches for minimum One Year or remove the Router & Switches line item because these item will be stuck the complete project please find the below few links where is clear communicated that worldwide Supply Delays Cause Long Lead Times for IT Hardware: 1. https://www.mirazon.com/supply-chain-delays-cause-long-lead-times-for-it[1]hardware/ [secure-web.cisco.com] 2. https://www.mirazon.com/supply-chain-delays-cause-long-lead-times-for-it[1]hardware/ [secure-web.cisco.com] 3. https://www.bbc.com/news/technology-56847518 [secure-web.cisco.com] 4. https://www.curvature.com/resources/blog/global-chip-shortage-predicted-to[1]last-into-early-2023/ [secure-web.cisco.com] 5. https://today.duke.edu/2021/09/global-computer-chip-shortage-causes-delays [secure-web.cisco.com] 6. https://www.bbc.com/news/business-58230388 [secure-web.cisco.com] 7. https://www.networkworld.com/article/3619210/chip-shortage-will-hit-it[1]hardware-buyers-for-months-to-years.html [secure-web.cisco.com] 8. https://www.whitehouse.gov/cea/written-materials/2021/06/17/why-the[1]pandemic-has-disrupted-supply-chains/ [secure- **We therefore request to you kindly consider the above clause also .**			Please be guided as per the RFP
210.	**HITACHI**		Minium Specification **Internet Router** Ports: 12x1/10GE WAN ports, 2X40GE and 2X40/100GE SPF/SPF+ base ports	Change Request Maxisum Specs is qulifiled sigle OEM Specific , request to kindly amend for fair compitition	Please refer to the Corrigendum

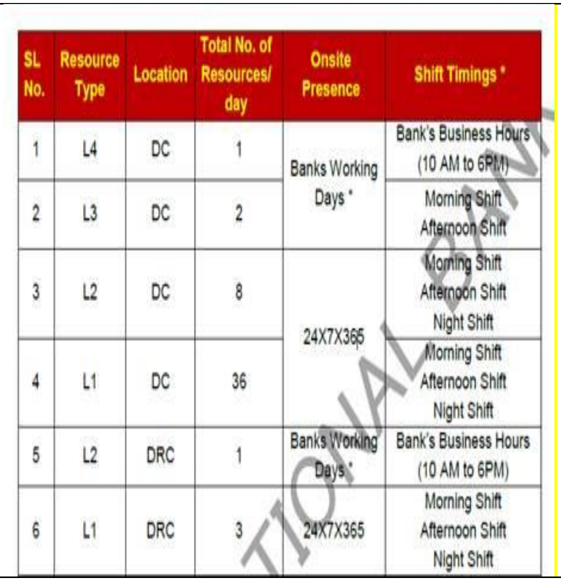
Line Cards	2 line cards with 10,40,100 Gigabit Ethernet ports
RAM	16GB and upgradable to 32 GB
Form Factor	1U(Preferably) in standard 42U Rack
Protocols	Pv4, IPv6, Static routes, RIP and RIPv2, OSPFv3, EIGRP, BGP, IGMPv3, IKE, ACL, DHCP, HSRP, RADIUS, AAA, IPv4-to-IPv6 Multicast, MPLS, Layer 2 and Layer 3 VPN, IPsec, MAC-Sec, SSHv2, SNMPv2c, SNMPv3, NTP, RADIUS, TACACS+
Encapsulations	GRE, Ethernet, 802.1q VLAN, PPP, HDLC, PPPoE
Encryptions/ Authentication	DES, 3DES, AES-128, AES-256, MD5, MD5, SHA, SHA-256, SHA-384, SHA-512
Supports SDWAN with IPSec Throughput – 30 Gbps	
Interconnect Switches	
Minimum Core Specification	
Ports	24/48 nos. 25G,40G SFP/SFP+/QSFP based ports with 100G SFP/SFP+/QSFP+ based uplink Ports
RAM	16GB
Protocols	IPv4, IPv6, static routing, RIP, PIM, OSPF, VRRP, PBR, QoS, BGPv4, BGPv6 , MPLS, VRF, VXLAN, ISISv4, OSPFv3, MP-BGP, SSHv2, SNMPv2c,

28x10GE ports, 6X40GE and 2X100GbE ports
Yes
64GB
8 U
EIGRP, HSRP are OEM specific. Kindly remove. Remove MAC-Sec and SNMPv2c
Remove it
Please remove DES, 3DES, AES-128, AES-256, MD5, MD5, SHA, SHA-256, SHA-384, SHA-512
Please remove "Supports SDWAN with IPSec Throughput – 30 Gbps"
Maxisum Specs is qulifiled sigle OEM Specific , request to kindly amend for fair compitition
48x10/25 SFP+ ports with 8X100G ports
64GB
Please remove 1588v2
Please remove IPv6 Binding Integrity Guard, IPv6 Snooping, IPv6 RA Guard, IPv6 DHCP Guard, IPv6 Neighbour Discovery Inspection
Please remove HA Active-Active/Active-Passive with Clustering

			SNMPv3, NTP, RADIUS, TACACS+ **Others Features:** IEEE 802.1D, 802.1s, 802.1w, 802.1x, 802.3ad, 802.3x, 802.1p, 802.1Q, 802.3, 802.3u, 802.3ab, 802.3z & 1588v2. IPv6 Binding Integrity Guard, IPv6 Snooping, IPv6 RA Guard, IPv6 DHCP Guard, IPv6 Neighbour Discovery Inspection and IPv6 Source Guard. HA Active-Active/Active-Passive with Clustering		
211.	**HITACHI**	Clause number 149"	Throughput scalability Clause number 149 page number 46 in published Corrigendum 1 is not revised/updated as per the response (Response published - Sl No.52 page number 13 in Corrigendum 1) Existing Clause: Original Tender *Inspection throughput- 100 Gbps* *IPsec VPN - 30 Gbps(AES256-SHA256)* *Sessions- 1,000,000 per second* *Concurrent Sessions -50M* As clarified in corrigendum 1: Refer Sl No.52 page number 13 Inspection throughput- 120 Gbps *IPsec VPN - 30 Gbps(AES256-SHA256)* *New Sessions- 3.2 Million per second* *Concurrent Sessions -50 Million*	As clarified in corrigendum 1: Refer Sl No.52 page number 13 Inspection throughput- 120 Gbps IPsec VPN - 30 Gbps(AES256-SHA256) New Sessions- 3.2 Million per second Concurrent Sessions -50 Million Revised clause still refers the pre-corrigendum numbers and thus creating a ambiguity on the throughput ask.Seeking clarification to propose the solution which adheres to the PNB ask and able to meet the scalabilty in future.	Please refer to the Corrigendum

			New Clause as per ANNEXURE-XI(A) in corrigendum 1: Refer clause number 149 page number 46 *Inspection throughput- 100 Gbps* *IPsec VPN - 30 Gbps(AES256-SHA256)* *Sessions- 1,000,000 per second* *Concurrent Sessions -50M* Revised clause still refers the pre-corrigendum numbers and thus creating a ambiguity on the throughput ask.Seeking clarification to propose the solution which adheres to the PNB ask and able to meet the scalabilty in future.		
212.	**HITACHI**	Clause number 148"	As per the RFP ask PNB Bank is looking for an upgrade to Next Generation Firewall .Please clarify if the inspection throughput asked in the clause number 148,149 on page number 46 in corrigendum 1 is NGFW throghput .We request Bank to please clarify to ensure that the proposed device meets the solution requirement.	As per the RFP ask PNB Bank is looking for an upgrade to Next Generation Firewall .Please clarify if the inspection throughput asked in the clause number 148,149 on page number 46 in corrigendum 1 is NGFW throghput .We request Bank to please clarify to ensure that the proposed device meets the solution requirement.	Please refer to the Corrigendum
213.	**HITACHI**	23	8X 10G ports (SFP + Fiber port), 4x 40G (QSFP + Fiber port) ports 2 x 1G RJ45 Management Port . Fail to wire switch along with proposed device with minimum 4 bypass segment/ or can be achieved through additional external switch populated with same interfaces capacity to achieve fail over or Achived through software by pass at interface level	8X 10G ports (SFP + Fiber port), 2x 40G (QSFP + Fiber port) ports 2 x 1G RJ45 Management Port . Fail to wire switch along with proposed device with minimum 4 bypass segment/ or can be achieved through additional external switch populated with same interfaces capacity to achieve fail over or Achieved through software by pass at interface level	Please refer to the Corrigendum
214.	**HITACHI**	71	Inspect SSL traffic for both RSA and ECC base key. Device should have support minimum 100,000 SSL TPS without session reuse for ECC & 2048 key RSA from day one and scalable up to 200,000 SSL TP S without hardware change	Request to remove this point as its specific to Application Delivery Controller and Load Balancer. As far as Anti-DDoS is concerned, SSL CPS specification is covered in original RFP Page 121 point # 63 and Corrigendum Page 40 point # 65	Please refer to the Corrigendum
215.	**HITACHI**	34	OEM shall provide scrubbing to mitigate unlimited number of attacks and has to ensure that the required legitimate throughput should always be available for the Bank.	Bidder/MSSP/ISP/OEM shall provide scrubbing services to mitigate unlimited number of attacks and has to ensure that the required legitimate throughput should always be available for the Bank.	Please refer to the Corrigendum

216.	**HITACHI**	106	Service should be always on	Service should be always on or On-Demand Protection	Please refer to the Corrigendum
217.	**HITACHI**	466	Store minimum 15(Fifteen) days full Raw packets and 90(ninety) Days of indexed Meta data, having usable disk capacity of minimum 300 TB for raw packets & 100 TB for indexed metadata separately, after RAID configurations respectively having minimum 4 Ports (2 X 1Gbps Copper and 2X10 Gbps Fiber) on capture appliance. Bidder may factor additional storage as per the requirement	The average calculation for storing 20 Gbps of sustained traffic throughput over 24 hours for 15 days would be 3.164 Petabytes. If we assume bank working hours for sustained throughout is 12 hours (which is an ideal assumption), the storage required would still be 1.5 Petabytes. In the RFP, you have asked only 300 TB for raw packets which covers just 10- 12% of your retention requirements. Also, you are asked to factor additional storage as per requirements, that means almost 90% of your retention requirements. Let us explain the storage calculations which is not any hidden formulae. You can also calculate it as explained below : Storage required in TB = ((((Throughput in Gbps/8)*3600) * sustained throughput peak in hours) * no of days retention required)/1024 Legend: Throughput in Gbps Throughput required to be monitored by Bank 8 No of bytes (conversion to size) to be generated 3600 Per hour size generated (60 seconds x 60 minutes) Sustained throughout peak in hours Assumption for no of peak sustained throughput hours – Based on work environment 1024 Convert total MB size in to TB Example scenario: For 12 hours sustained 20-Gbps peak throughput below is the	Please refer to the Corrigendum

<table>
<tr><td></td><td></td><td></td><td></td><td>formulae for storage calculation: Storage required in TB =((((20/8)*3600)*20)*15)/1024 which equals to 1582 TB.
In this context, we request you to ensure the retention storage size asked as per actual calculations to ensure bidders provide the minimum requirements required to achieve the retention period storage. Please help revise the storage requirements clause to actual requirements to help ensure bank does not end up in under supply or compromise on storage solution as SI's bid will refer to listed numbers in RFP and commercial Bill of materials clauses.</td><td></td></tr>
<tr><td>**218.**</td><td>**INSPIRA ENTERPRISE**</td><td>Shift Planning of Resources</td><td>
<table>
<tr><th>SL No.</th><th>Resource Type</th><th>Location</th><th>Total No. of Resources/ day</th><th>Onsite Presence</th><th>Shift Timings *</th></tr>
<tr><td>1</td><td>L4</td><td>DC</td><td>1</td><td>Banks Working Days *</td><td>Bank's Business Hours (10 AM to 6PM)</td></tr>
<tr><td>2</td><td>L3</td><td>DC</td><td>2</td><td></td><td>Morning Shift
Afternoon Shift</td></tr>
<tr><td>3</td><td>L2</td><td>DC</td><td>8</td><td>24X7X365</td><td>Morning Shift
Afternoon Shift
Night Shift</td></tr>
<tr><td>4</td><td>L1</td><td>DC</td><td>36</td><td></td><td>Morning Shift
Afternoon Shift
Night Shift</td></tr>
<tr><td>5</td><td>L2</td><td>DRC</td><td>1</td><td>Banks Working Days *</td><td>Bank's Business Hours (10 AM to 6PM)</td></tr>
<tr><td>6</td><td>L1</td><td>DRC</td><td>3</td><td>24X7X365</td><td>Morning Shift
Afternoon Shift
Night Shift</td></tr>
</table></td><td>"Kindly confirm the number of L1 resources (36 at DC & 3 at DRC) to be deployed at DC and RDC in each shift.
As per our understanding 12 L1 engineer to be deployed in each shif t i.e. Morning Shift, Afternoon Shift and Night Shift.
Kindly confirm."</td><td>Please be guided as per the RFP</td></tr>
<tr><td>**219.**</td><td>**INSPIRA ENTERPRISE**</td><td>SCORING METHODOLOGY</td><td>Marks on resources experience –
1. 1 marks for minimum 10 CCIE/CISSP in the organisation for experience of minimum 5 years.
2. 0.5 mark per CCIE/CISSP certified resource above 10 resources having experience of more than 5 years
(Undertaking along with duly Bio Data of onsite resource experience to be submitted. Employee should be on company payroll)</td><td>As per the manpower skillset mentioned in the RFP, only L4 and L3 resources are asked to be CCIE/CISSP certified. And the total requirement of L4 and L3 resouces are 1 and 2 respectively.
But in Scoring Methodology you have asked that bidders should have at least 10</td><td>Please be guided as per the RFP</td></tr>
</table>

				CCIE/CISSP certified reosurces to obtain 1 marks. And in order to obtain a maximum marks of 5 bidder has to submit the details of at least 50 CCIE/CISSP certified resources. We request you to kindly relax and amend this clause as: 5 marks for minimum 5 CCIE/CISSP in the organisation for experience of minimum 5 years.	