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

Corrigendum 1: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component

<table>
<tr><th>Sl No.</th><th>RFP Page No</th><th>RFP Clause No</th><th>RFP Clause</th><th>Existing Clause in RFP</th><th>New Clause in RFP</th></tr>
<tr><td>1.</td><td></td><td>4. SOW</td><td>Security Analyst Level 4 (L4):</td><td>Addition</td><td>a. Create the fresh design document as per the physical deployment of network security architecture of DC/DR/NEAR DR
b. Re-design the network security architecture of DC/DR/NEAR DR as per the best practices. Same will be deployed after obtaining approval from the Bank</td></tr>
<tr><td>2.</td><td>74</td><td>9.</td><td>TIMELINE & PENALTY</td><td>
<table>
<tr><th>Deliverables</th><th>Timelines</th><th>Penalty</th><th>Maximum Penalty</th></tr>
<tr><td>Deployment of Onsite FM engineer after release of P.O.</td><td>Within 30 Days from date of Purchase Order (P.O.)</td><td>1% of (B) for every week’s delay or part there of</td><td rowspan="2">Upto 10% of (A+B+C+D+E+F)</td></tr>
<tr><td>Delivery of Devices and applicable Licenses, wherever applicable after release of P.O. ,</td><td>Within 12 weeks from date of Purchase Order (P.O.)</td><td>1% of (A+E) for every week’s delay or part there of</td></tr>
</table>
</td><td>
<table>
<tr><th>Deliverables</th><th>Timelines</th><th>Penalty</th><th>Maximum Penalty</th></tr>
<tr><td>Deployment of Onsite FM engineer after release of P.O.</td><td>Within 60 Days from date of Purchase Order (P.O.)</td><td>1% of (B) for every week’s delay or part thereof</td><td rowspan="2">Upto 10% of (A+B+C+D+E+F)</td></tr>
<tr><td>Delivery of Devices and applicable Licenses, wherever applicable after release of P.O. ,</td><td>Within 18 weeks from date of Purchase Order (P.O.)</td><td>1% of (A+E) for every week’s delay or part thereof</td></tr>
</table>
</td></tr>
</table>

				Installation & Integration of Devices, Sign-off, Contract signing.	Within 20 weeks from P.O date	1% of (A+B +E) for every week' s delay or part there of		Installation & Integration of Devices, Sign-off, Contract signing.	Within **32 weeks** from P.O date	1% of (A+B+ E) for every week's delay or part thereof	
3.	**72-73**	**10.**	**TIMELINE & PENALTY**	**Deliverables**	**Timelines**			**Deliverables**	**Timelines**		
				Deployment of initial Onsite FM engineers after release of PO	Within 30 Days from date of Purchase Order (P.O.)			Deployment of initial Onsite FM engineers after release of PO	Within **60** Days from date of Purchase Order (P.O.)		
				Completion of all formalities and signing of Contract - Service Level Agreement with the Bank	Within 30 Working Days from date of Purchase Order (P.O.)			Completion of all formalities and signing of Contract - Service Level Agreement with the Bank	Within **30 Working Days** from date of Purchase Order (P.O.)		
				Delivery of all Devices and applicable Licenses, wherever applicable after release of P.O.	Within 12 weeks from date of Purchase Order (P.O.)			Delivery of all Devices and applicable Licenses, wherever applicable after release of P.O.	Within **18 weeks** from date of Purchase Order (P.O.)		
				Deployment of all OTS/ SI Resources as per P.O	Within 20 weeks from date of Purchase Order (P.O.) or on the day of signoff, whichever is earlier			Deployment of all OTS/ SI Resources as per P.O	Within 20 weeks from date of Purchase Order (P.O.) or on the day of signoff, whichever is earlier		
				Installation & Integration of all the Devices & Go-live of entire solution,	Within 20 weeks from date of P.O			Installation & Integration of all the Devices & Go-live of entire solution,	Within **32 weeks** from date of P.O		

				Sign-off,	After 90 days from signoff	Sign-off,	After **90 days** from signoff	
4.	**49**	**Other Conditions**		More than 2 SIs of the Principal/OEM/ Solution Provider cannot bid for the same product. All proposed L4 and L3 and 50 % of L2 engineers as per PO, must be on the company roll for a minimum period of six months on the similar scope of work. All other L2 and L1 engineers should be on company payroll. Resources from franchise/partners on outsourcing model are not acceptable. All resources should clear interview process by Bank officials/Bank appointed consultants. Before replacing/changing the existing resources, a minimum 2-month notice is required and Bank's consent is to be obtained.		**All engineers, must be on the company roll on the similar scope of work. Resources from franchise/partners on outsourcing model are not acceptable. All resources should clear interview process by Bank officials/Bank appointed consultants. Before replacing/changing the existing resources, a minimum 2-month notice is required and Bank's consent is to be obtained.**	
5.	**79**	**10**	**SLA**	All proposed L4 and L3 and 50 % of L2 engineers as per PO, must be on the company roll for a period of minimum six months on the similar scope of work. All other L2 and L1 engineers should be on company payroll. Resources from franchise/partners on outsourcing mode are not acceptable. All resources should clear interview process by Bank officials/Bank appointed consultants. Before replacing/changing the existing resources, a minimum 2-month notice is required and Bank's consent is to be obtained.		**All engineers, must be on the company roll on the similar scope of work. Resources from franchise/partners on outsourcing model are not acceptable. All resources should clear interview process by Bank officials/Bank appointed consultants. Before replacing/changing the existing resources, a minimum 2-month notice is required and Bank's consent is to be obtained.**	
6.	18	SOW, Supply, Implementation and Management of New devices:	Clause a)	All the proposed devices to be supplied as a part of this RFP should be running with similar or higher configuration in any organization for atleast one year. Bidder has to provide supporting documents like Purchase Order (P.O) copy and Performance Certificate.		All the proposed devices to be supplied as a part of this RFP should be **implemented/supplied by the OEM with similar configuration in any organization in India.** Bidder has to provide supporting documents like Purchase Order (P.O) copy and Performance Certificate. **Incase a previous iteration of the same hardware is referenced for this purpose, a certificate from the OEM validating the same should be provided.**	
7.	21	3. Network Intrusion Prevention System (NIPS) (zero day, signature based prevention also inbuilt TLS decryptor)		The solution should have inbuilt TLS/SSL decryptor to inspect encrypted traffic and prevent attacks		The solution should have inbuilt / **external** TLS/SSL decryptor to inspect encrypted traffic and prevent attacks		

8.	26	SOW	9. Multi Factor Authentication	Proposed MFA solution should be hardware based base and deployed on-premises	Proposed MFA solution should be hardware based or **software based with underlying hardware infra** and deployed on-premises
9.	50	Instruction to Bidders	Clause 1. POWER OF ATTORNEY/ AUTHORIZATION LETTER OR RESOLUTION COPY	In case of company, Board Resolution in favor of Authorized Person and Power of Attorney/Authorization letter (from authorized person executed on stamp paper of appropriate value), in case the authorized person delegates authority to another person of the company to sign the Bid documents, is to be submitted with bid documents for all the OEMs and bidder involved in the Bid.	In case of company, **a certified copy of the latest** Board Resolution in favor of Authorized Person(s) **duly authorized by the Company Secretary/ Director along with validity of the authorization is to be submitted AND** in case the authorized person delegates authority to another person of the company to sign the Bid documents, **Power of Attorney in original (from authorized person executed on stamp paper of appropriate value) with bid reference, showing that the signatory has been duly authorized to sign the bid documents, execute contract/agreements with the Bank on behalf of the company**
10.	103	Eligibility Criteria, Annexure III	SL No. 3	The bidder should be an OEM of the components/devices/software etc. offered or its authorized representative or authorized partner (Tier 1/ Gold/ Platinum) in India having IP Rights of the customization wherever applicable.	The bidder should be an OEM of the components/devices/software etc. offered as a part of this RFP or its authorized representative or authorized partner (Tier 1/ Gold/ Platinum/ **Silver**) in India
11.	103	Eligibility Criteria, Annexure III	Sl No. 4	The bidder must be CMMI level 3 or above Certified Company and the certificate should be valid as on date of bid submission.	Clause stands deleted
12.	103	Eligibility Criteria, Annexure III	Sl No. 4	Bidder should be an ISO certified Company in terms of Quality of Services & Information Security Standards. Certified copy of ISO 27001:2013 (or later) & ISO 9001:2008 (or later) certificates	Bidder or their parent or their group of companies should be an ISO certified Company in terms of Quality of Services & Information Security Standards. Certified copy of ISO 27001:2013 (or later)
13.	103	Eligibility Criteria, Annexure III	SL No. 5	Bidder should have a minimum 5 years' experience in implementing Information Security Products and Services either as security integrator or as security implementer including deployment of SOC in large financial institutions which has its offices/branches in atleast 2 of the Metro cities- Delhi NCR, Mumbai , Chennai, Bangalore, Kolkata and Hyderabad with wide area network, intranet and internet as well as demilitarized zone and security equipment's like (atleast 3) Next Generation Firewalls, NIPS, Application delivery controller(ADC), Web Application Firewall(WAF) etc. Out of 5 years' experience, at least 3-year experience (as on the date of publishing this RFP) should be in a	Bidder should have minimum 5 years' experience in implementing Information Security Products and Services either as security integrator or as security implementer including deployment of SOC in large financial institutions which has its offices/branches in atleast 2 of the Metro cities- Delhi NCR, Mumbai , Chennai, Bangalore, Kolkata and Hyderabad with wide area network, intranet and internet as well as demilitarized zone and security equipment's like (atleast 3) Next Generation Firewalls, NIPS, Application delivery controller(ADC), Web Application Firewall(WAF) etc. Out of 5 years' experience, at least 3-year experience (as on the date of publishing this RFP) should be in a Scheduled Commercial Banks with minimum **1.4** Lakh Crores total business in FY 2020-21 or 2021-22 or RBI

				Scheduled Commercial Banks with minimum 2 Lakh Crores total business in FY 2020-21 or 2021-22	
14.	103	Eligibility Criteria, Annexure III	SL No. 6	The Bidder should have successfully executed at least three projects in either – ·Designing of Information Security architecture, ·System integration of IT Security solution/ Information security OR · Security Operations Centre(SOC/CSOC) components in India Out of these 3: 1. At least Two should be in BFSI segment. 2. At least one Project of value not less than ₹ 15 Crores in India/- (₹ Fifteen Crores only)	The Bidder should have successfully executed at least three projects in either – ·Designing of Information Security architecture, ·System integration of IT Security solution/ Information security OR · Security Operations Centre(SOC/CSOC) components in India Out of these 3: 1. At least Two should be in BFSI segment. 2. At least one Project of value not less than ₹ **5** Crores in India/- (₹ Five Crores only)
15.	104	Eligibility Criteria, Annexure III	Sl No. 10	All the products offered as a part of this RFP should have been implemented in at least one Organization with same or higher core specifications. These installations should be live for at least one year as on the date of publishing this RFP.	All the proposed devices to be supplied as a part of this RFP should be **implemented/supplied by the OEM with similar configuration in any organization in India.** Bidder has to provide supporting documents like Purchase Order (P.O) copy and Performance Certificate. **Incase a previous iteration of the same hardware is referenced for this purpose, a certificate from the OEM validating the same should be provided.**
16.	105	Eligibility Criteria, Annexure III	Note, Sl No.1	In case of OEM or it's Indian Authorized Representative (IAR) / Agent / System Integrator (SI), maximum two Authorized Representatives of a particular Principal or Original Equipment Manufacturer (OEM) / Solution Provider can participate in the tender process.	Clause stands deleted
17.	105	Eligibility Criteria, Annexure III	SL No. 20	Power of Attorney and Copy of Board Resolution to prove authorized signatory of Bidder.	In case of company, **a certified copy of the latest** Board Resolution in favor of Authorized Person(s) **duly authorized by the Company Secretary/ Director along with validity of the authorization is to be submitted AND** in case the authorized person delegates authority to another person of the company to sign the Bid documents, **Power of Attorney in original (from authorized person executed on stamp paper of appropriate value) with bid reference, showing that the signatory has been duly authorized to sign the bid documents, execute contract/agreements with the Bank on behalf of the company**
18.	105	Eligibility Criteria, Annexure III	SL No. 20	Performance Certificate & P.O. supporting the claim from the respective organization should be submitted along with contact details of the company.	**Satisfactory Performance Certificate from the Clients strictly as per Annexure-VI and masked PO supporting the same** **OR** **Copy of Work Order/PO along with Confirmation Mail from the Client (as per contents in Annexure VI) stating that the work order has been successfully executed** **OR**

					Copy of Work Order along with Installation Certificate signed & stamped by the Client **OR** **Copy of Work Order along with any other proof of execution.** **(Kindly note that any of the above documents submitted must be sufficient enough to certify bidder's experience, must be authentic and must also contain all the material information as required in Annexure-VI). Clients contact details (E-Mail ID and Contact number must be provided for verification, if required by the Bank)**
19.	118	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 ROUTER	SL No. 3. Power on Demand	Redundant 4 AC/DC power supplies	**Atleast 2** Redundant AC/DC power **supply**
20.	119	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 SWITCH	SL No. 19, Ports	24/48 nos. 25G,40G SFP/SFP+/QSFP based ports with 100G SFP/SFP+/QSFP+ based uplink Ports	24/48 nos. **25G/40G** SFP/SFP+/QSFP based ports with 100G SFP/SFP+/QSFP+ based uplink Ports
21.	120	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 Anti DDoS/DDoS Preventive Module	Sl No. 33. Throughput	Inspection and Mitigation: 20 Gbps Layer 4: 25 Gbps 100 Million L4 and Hardware sync DDoS Flood Attack Prevention Rate: 20 Mpps DDoS Cloud Mitigation: 5 Gbps	Inspection and Mitigation: 20 Gbps DDoS Flood Attack Prevention Rate: **Minimum 30 Mpps** DDoS Cloud Mitigation: **4 Gbps**
22.	120	Annexure XI(A) TECHNICAL AND FUNCTIONAL	SL No. 34. Throughput	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	Inspection and Mitigation: 40 Gbps (without additional hardware) Attack Prevention Rate: **39 Mpps** without hardware change (This performance figure must be mentioned in public facing datasheet) DDoS Cloud Mitigation: 20 Gbps

		SPECIFICATIONS OF THE SOLUTION, Table 1 Anti DDoS/DDoS Preventive Module	Scalability	mentioned in public facing datasheet). DDoS Cloud Mitigation: 20 Gbps	
23.	120	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 Anti DDoS/DDoS Preventive Module	SL No. 37. Ports	8X 10G ports (SFP + Fiber port), 6 x 40G (SFP + Fiber port) ports. 4 x 10GBASE-SR and 4 x 1GBASE-T Transceivers for each appliance. Fail to wire switch along with proposed device with minimum 4 bypass segment	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**
24.	120	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 Anti DDoS/DDoS Preventive Module	SL No. 40	Proposed product/solution should be stateless Technology not having any kind of state limitation e.g. TCP connections.	Proposed product/solution should be stateless Technology not having any kind of state limitation e.g. TCP connections OR Proposed DDoS product/solution should be stateless in nature
25.	120	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 Anti DDoS/DDoS Preventive Module	Sl No. 42	Work in fail open mode in all the ports and should support software bypass capability	Work in fail open or **fail close** mode in all the ports or should support software bypass capability **or should be achieved through additional external switch populated with same interfaces capacity**
26.	120	Annexure XI(A) TECHNICAL AND	SL No. 46	Inbuilt mechanism to inspect traffic with external threat feed and shall support at least 3Million IOC's for inline blocking (URL/ Hash / domain / IP address / subnet)	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)

		FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 Anti DDoS/DDoS Preventive Module			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**
27.	121	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 Anti DDoS/DDoS Preventive Module	SL No. 65	Ability to limit the number of connections depending on source or range	Clause stands deleted
28.	120	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 Anti DDoS/DDoS Preventive Module	SL No. 39	1U(Preferably) in standard 42U Rack	1U/**2U**(Preferably) in standard 42U Rack
29.	120	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 Anti DDoS/DDoS Preventive Module	Sl No. 49	Support integration of external Threat Intelligence Platform (TIP)	Support integration of external Threat Intelligence Platform (TIP) **OR Support Threat Intelligence Feed**
30.	121	Annexure XI(A) TECHNICAL	Sl No. 60	Support comprehensive countermeasure to protect against zero-day attack, Challenge - Response Mechanism, and	Support comprehensive countermeasure to protect against zero-day attack, Challenge - Response Mechanism, and which should be able

		AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 Anti DDoS/DDoS Preventive Module		which should be able to Detect and protect attacks in real time through inbuilt Captcha Mechanism	to Detect and protect attacks in real time through inbuilt Captcha Mechanism **or HTTP Authentication**
31.	121	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 Anti DDoS/DDoS Preventive Module	SL No. 78	Built-in hardware bypass for all interface types	Built-in hardware bypass **or software bypass** for all interface types
32.	121	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 Anti DDoS/DDoS Preventive Module	SL No. 83	Cloud signaling to signal to upstream ISPs or managed service provider who is providing anti-DDoS cloud service for very large DDoS attack mitigation.	The proposed DDoS Solution must support cloud signaling to signal to upstream ISPs or managed service provider who is providing anti-DDoS cloud service for Volumetric DDoS attack mitigation. The on-premise DDoS appliance should integrated with at-least 4 ISP's Scrubbing center solution in India, appropriate proof needs to be submitted
33.	122	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 Anti DDoS/DDoS Preventive Module	SL No. 101	Proposed solution should Protect against SSL & TLS-encrypted information leaks with an separate SSL Decryption module on device / out of Path	Clause stands deleted

34.	122	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 Anti DDoS/DDoS Preventive Module	SL No. 105	Bandwidth should be dedicated and not shared. Connectivity required, if any, will have to be arranged and factored by the bidder.	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.
35.	122	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 Anti DDoS/DDoS Preventive Module	SL No. 91	The Device must have an updated IP reputation feed that describes suspicious traffic Blacklisted IPs, botnets, Phishing. It should be updated every minute to block and protect network against active attackers. Same may be facilitated integrate with its proprietary Threat intelligence or may take feed from reputed Threat intelligence experts which can provide compliance to points mentioned sub paras(the commercial for external/internal threat intelligence feed should be factored in commercial section for 5 years)	The Device must have an updated IP reputation feed that describes suspicious traffic Blacklisted IPs, botnets, Phishing. It should be updated **atleast once hourly** to block and protect network against active attackers. Same may be facilitated integrate with its proprietary Threat intelligence or may take feed from reputed Threat intelligence experts which can provide compliance to points mentioned sub paras (the commercial for external /internal threat intelligence feed should be factored in commercial section for 5 years)
36.	122	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 Anti DDoS/DDoS Preventive Module	Sl No. 97	System should disclose time to mitigation from detection of attack for all types of attack including known and unknown attacks	Clause stands deleted
37.	122	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NIPS	SL No. 109, Throughput	System:20 Gbps (with all features enabled) SSL Inspection: 18 Gbps with 1,300,000 SSL flow count Maximum Concurrent connections: 13,000,000	System:20 Gbps (with all features enabled) **with mix traffic inspection**

38.	122	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NIPS	SL No. 112, Ports	Fixed 4-10G copper ports fixed ports with fail open and 8 - 40G QSFP+ fiber ports with fail open Dedicated 1 (1G / 100M)port for management console	Minimum of 4**X**10G copper ports with fail open and 6**X**40G QSFP+ fiber ports with fail open Dedicated 1 (1G / 100M)port for management console
39.	123	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NIPS	SL No. 113, Form Factor	1U(Preferably) in standard 42U Rack	1U/**2U** in standard 42U Rack
40.	123	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NIPS	SL No. 114, Gartner Magic Quadrant	Part of Leaders quadrant of last published Gartner MQ for 3 consecutive years.	Clause stands deleted
41.	123	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NIPS	SL No. 115	NIPS solution should be a purpose built dedicated standalone appliance and not an integrated firewall module or UTM appliance. NIPS should be from different manufacturer as of Networking (Router-Switch) & Firewall OEMs.	Clause stands deleted
42.	123	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NIPS	SL No. 116	Monitoring Interface should be able to operate at layer 2.	Clause stands deleted
43.	123	Annexure XI(A) TECHNICAL AND	SL No. 118	NIPS should support different mode of deployment. · IDS · TAP Mode	NIPS should support different mode of deployment. · IDS · TAP Mode

		FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NIPS		· Inline · Simulation	· Inline · Simulation**(Optional)**
44.	123	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NIPS	SL No. 133	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
45.	124	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NIPS	SL No. 137	Communication fabric based integration with multiple other existing solution hunting solution in a way that it can share the telemetry data for predictive analysis.	Clause stands deleted
46.	124	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NIPS	SL No. 140	Inbound SSL Inspection detection and prevention using dynamic agent based key for ECDHA cypher suits	Inbound SSL Inspection detection and prevention using ECDHA **or ECDHE** cypher suits
47.	124	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NIPS	SL No. 146	Communication fabric based integration with multiple other existing solution of PNB such as immediately share relevant data between endpoint, gateway, and other security products enabling security intelligence and adaptive security.	Clause stands deleted
48.	124	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE	SL No. 147	Inbuilt network behavioural analysis engine to provide additional context using network flows.	**OPTIONAL**: Inbuilt network behavioral analysis engine to provide additional context using network flows.

		SOLUTION, Table 1 NIPS			
49.	124	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NIPS	SL No. 153	Management console should have the ability to allow access to specific hosts by enabling GUI Access and defining the list of authorized hosts/networks	Management console should have the ability to allow access to specific hosts**/users** by enabling GUI Access and defining the list of authorized hosts**/users**
50.	124	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NIPS	SL No. 160	OEM Engineering and Support for the NIPS solution should be based out of India.	Clause stands deleted
51.	125	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NGFW	SL No. 164, Storage	512 GB in in Raid 1 for system and 2 TB for Logging capability	Minimum **400 GB SSD** for system and 2 TB SSD for Logging capability
52.	125	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NGFW	SL No. 166, Throughput Scalability	Inspection throughput- 100 Gbps IPsec VPN - 30 Gbps(AES256-SHA256) Sessions- 1,000,000 per second Concurrent Sessions -50M	Inspection throughput- 120 Gbps IPsec VPN - 30 Gbps(AES256-SHA256) New Sessions- 3.2 Million per second Concurrent Sessions -50Million
53.	125	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NGFW	SL No. 167, Latency	<=12 microseconds ,(64 byte UDP)	Clause stands deleted

54.	125	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NGFW	SL No. 170, Ports	10x25Gig SFP/SFP+ ports with respective SR transceivers & 2 x 40G QSFP28 ports with respective transceivers 2x HA ports 4 x 25/40/100G SFP interfaces and 20x10 Gigabit SFP OOB, Console Management USB Port 4 X 1/10 Gig	**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
55.	125	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NGFW	SL No. 171, Firewall Policies	50,000 with an additional upgradation capacity of 50,000 without any additional hardware	**Atleast 50,000**
56.	125	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NGFW	SL No. 175	Routing protocols: Static, RIP v2, OSPFv2/v3 , BGP v4, DNS service providers: DuckDNS, DynDNS, FreeDNS Afraid.org Dynamic API, FreeDNS Afraid.org, and No-IP. Mobile protocols : GTP, SCTP, etc. and support for termination of GRE Tunnels 1000 VLANs	Static, RIP v2, OSPFv2/v3 , BGP v4. The Next Generation Firewall must support DDNS including integration with third party DNS service providers : Mobile protocols : GTP, SCTP, etc. and support for termination of GRE Tunnels 1000 VLANs
57.	125	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NGFW	Sl No. 176, Gartner Magic Quadrant	Part of Leaders quadrant of last published Gartner MQ for 3 consecutive years.	Clause stands deleted
58.	126	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NGFW	SL No. 183	Solution should be on multi-core architecture and must not be an ASIC based solution.	Clause stands deleted
59.	126	Annexure XI(A) TECHNICAL AND	SL No. 185	Minimum NG Threat prevention throughput in real world/production/Application Mix environment (by enabling and measured with Application-ID/AVC, User-ID/Agent-ID,	Minimum NG Threat prevention throughput in real world/production/Application Mix environment (by enabling and measured with Application-ID, AVC, NGIPS, Anti-Virus, Anti-

		FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NGFW		NGIPS, Anti-Virus, Anti-Spyware, zero-day attack prevention and file blocking security threat prevention features 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	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.
60.	127	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NGFW	SL No. 208	Integrated IPS capabilities with minimum 20000+ signature database. It should support importing signatures from Third party tools, customizing IPS signature and creation of multiple IPS policy for different segments and zones	Integrated IPS capabilities with minimum **10000+** signature database. It should support importing signatures from third party tools, customizing IPS signature and creation of multiple IPS policy for different segments and zones.
61.	127	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NGFW	SL No. 213	Perform Anti-virus scans for HTTP, smtp, imap, pop3, ftp, SMB traffic with configurable AV action such as allow, deny, reset, alert etc.	Perform Anti-virus scans for HTTP, smtp, imap, pop3, ftp, SMB traffic with configurable AV action such as allow, deny, alert etc.
62.	127	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NGFW	SL No. 214	Should have DNS sink holing for malicious DNS request from inside hosts to outside bad domains and should be able to integrate and query third party external threat intelligence databases to block or sinkhole bad IP address, Domain and URLs	Clause stands deleted
63.	128	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NGFW	SL No. 224	Add custom threat prevention signature in an automated way by converting Snort and Suricata signatures into custom threat signatures.	Add custom threat prevention signature in an automated way by converting Snort **or** Suricata signatures into custom threat signatures.
64.	129	Annexure XI(A) TECHNICAL AND	SL No. 241	The solution must be able to use AV and zero day signatures based on payload and not just by hash values and it should support bare metal analysis if required. The advanced	**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 (malware

		FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NGFW		malware analysis (malware sandboxing) solution must have MacOS and Linux executable scanning by default.	sandboxing) solution must have MacOS and Linux executable scanning by default.
65.	129	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NGFW	SL No. 244	Cloud base unknown malware analysis service should be certified with SOC2 or any other Data privacy compliance certification for customer data privacy protection which is uploaded to unknown threat emulation and analysis	Clause stands deleted
66.	129	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NGFW	SL No. 245	This solution should be on premise whereas there should be option for hybrid malware analysis service with guaranteed protection signature delivery time not more than 5 minutes. This should be mentioned on the public datasheets or reference with cloud in India.	Clause stands deleted
67.	129	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NGFW	SL No. 247	Advance unknown malware analysis engine with real hardware, detecting VM-aware malware to detect and protect from virtual sandbox evading advance unknown malware. The device should support 28 VMs and at least 2X 8TB in RAID1	Advance unknown malware analysis engine with real hardware, detecting VM-aware malware to detect and protect from virtual sandbox evading advance unknown malware. The device should support **24 VMs** and at least **2X 2TB** in RAID1
68.	129	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NGFW	SL No. 249	Cloud base unknown malware analysis service should be able to perform dynamic threat analysis on such as EXEs, DLLs, ZIP files, PDF documents, Office Documents, Java®, Android APKs, Adobe Flash applets, Web pages that include high-risk embedded content like JavaScript, Adobe Flash files. MAC OS and DMG file types	Clause stands deleted
69.	129	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE	SL No. 250	Able to detect and prevent zero day threats infection through HTTP, HTTPS, FTP, SMTP, POP3, IMAP use by any of application used by the users (e.g.: Gmail, Facebook, MS outlook)	Able to detect and prevent zero day threats infection through HTTP, HTTPS, FTP, SMTP, IMAP use by any of application used by the users (e.g.: Gmail, Facebook, MS outlook)

		SOLUTION, Table 1 NGFW			
70.	129	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NGFW	SL No. 253	The protection signatures created base unknown malware emulation should be payload or content base signatures that cloud block multiple unknown malware that use different hash but the same malicious payload.	The protection signatures created base unknown malware emulation should be payload or content base signatures **or STIX format** that cloud block multiple unknown malware that use different hash but the same malicious payload.
71.	129	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NGFW	SL No. 258	Equipment Test Certification: FCC Class A, CE Class A, VCCI Class A, CB and Common Criteria Certified.	Equipment Test Certification: FCC Class A, CE Class A, VCCI Class A, CB **or** Common Criteria Certified.
72.	125	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NGFW	SL No. 165, Throughput	Inspection throughput- 50 Gbps IPsec VPN - 15 Gbps(AES256-SHA256) Sessions-615,000 per second Concurrent Sessions -20M	Inspection throughput- **30 Gbps** IPsec VPN - 15 Gbps(AES256-SHA256) New Sessions-615,000 per second Concurrent Sessions -20M
73.	125	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NGFW	SL No. 174, Form Factor	1U(Preferably) in standard 42U Rack	**Maximum 5U(Preferably)** in standard 42U Rack
74.	130	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NGFW	SL No. 265	SSL automatic exclusions for pinned applications.	Clause stands deleted

75.	130	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NGFW	SL No. 268	Support · Network Address Translation (NAT) · Port Address Translation (PAT) · Dual Stack IPv4 / IPv6 (NAT64, NPTv6)	Support · Network Address Translation (NAT) · Port Address Translation (PAT) · Dual Stack IPv4 / IPv6 (NAT64)
76.	130	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NGFW	SL No. 269	Support IPv6-: · Dynamic IP reservation · Tunable dynamic IP · Port oversubscription · Firewall policy with User and Applications · SSL Decryption · Administration of Gateway and Management solutions · DHCP · ECMP	Support IPv6-: • Port oversubscription • Firewall policy with User and Applications • SSL Decryption • Administration of Gateway and Management solutions • DHCP • ECMP
77.	130	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NGFW	SL No. 270	FQDN instead of IP address for static route next hop, policy based forwarding next hop and BGP peer address	Clause stands deleted
78.	130	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NGFW	SL No. 272	Load balancing of traffic on multiple WAN links based on application, latency, cost and type	Clause stands deleted
79.	130	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NGFW	SL No. 273	The proposed solution must support Policy Based forwarding based on: - Zone - Source or Destination Address - Source or destination port - Application (not port based) - AD/LDAP user or User Group - Services or ports	The proposed solution must support Policy Based forwarding/ Policy based Routing based on: - Zone - Source or Destination Address - Source or destination port - Application (not port based) - AD/LDAP user or User Group - **Services or ports**
80.	131	Annexure XI(A) TECHNICAL	SL No. 284	Provision to permanently block the export of private keys for certificates that have been generated or imported to harden	Clause stands deleted

		AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NGFW		the security posture in order to prevents rogue administrators from misusing keys.	
81.	131	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 ADC	SL No. 293, CPU	24 Core	24 **Physical** Cores
82.	131	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 ADC	SL No. 295	Dual Hot swappable SSD	**SSD Storage with minimum 500GB. Bidder/OEM may increase the size depending upon box capacity**
83.	131	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NGFW	SL No. 282	Ability to configure, manage and monitor NGFW using CLI and GUI both without central management solution. Bank would like to have full feature parity of centralized management tool on the Next Generation Firewall itself, in case there is any connectivity issues between Next Generation Firewall and central management tool or failure in central management tool	Clause stands deleted
84.	132	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 ADC	Sl No 298, Power on Demand	Hot Swappable redundant power supply and fan	Hot Swappable redundant power supply
85.	133	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIO	Sl No. 317	ICAP integration with other security devices for file vulnerability, virus, Trojan scanning during file submission with web-applications to improve security.	**Support ICAP integration with other security devices to improve security.**

		NS OF THE SOLUTION, Table 1 ADC			
86.	133	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 WAF	SL No. 332, Storage	Dual Hot swappable SSD. 960GB	**Minimum SSD Storage: 500GB**
87.	133	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 WAF	SL No. 336, Power on Demand	Hot Swappable redundant power supply and fan	Hot Swappable redundant power supply
88.	133	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 WAF	SL No. 338, Ports	10x10G BASE-SR SFP+ with 2 bypass 8X10/100/1000 Interface Ports	4*100G ports and 16*25G/10G with negotiable to 10G with SFP+/ QSFP+ as per the compatible interfaces
89.	134	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 WAF	Sl No. 353	The WAF solution should be enterprise grade and have been in the Gartner's Leaders or Magic Quadrant for "Web Application Firewall" in latest report.	Clause stands deleted
90.	135	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 WAF	SL No. 331, RAM	128 GB	**256 GB**

91.	135	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 WAF	SL No. 372	Able to encrypt the user credentials in real time i.e., when the user is typing the credentials for the web application in his/her browser for any web application that is behind the WAF. This feature should be agentless and should not require installation of any kind of software either on client end or on the application end.	Clause stands deleted
92.	135	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 WAF	SL No. 378	Automatically update Certificate bundles from the appropriate CAs without any user intervention.	**a)** Automatically update Certificate bundles from the appropriate CAs without any user intervention **OR** **b) Appliance should maintain certificate and key repository**
93.	135	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 WAF	SL No. 379	The solution must be able to encrypt the user credentials of the protected applications in real time by encrypting the password without any agent either on the client side or on the server side. This feature could be activated at any time with additional license on the WAF when required.	Clause stands deleted
94.	136	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 WAF	SL No. 396	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.	**OPTIONAL:** 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.
95.	136	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 WAF	SL No. 402	The solution support role-based admin access with roles like no access, Guest, Operator, Application editor, Resource Administrator and Administrator.	The solution support role-based admin access with roles like no access, Guest, Operator, Application editor, Resource Administrator, Administrator **or equivalent to achieve the objective**
96.	136	Annexure XI(A) TECHNICAL AND	SL No. 403	Able to secure synchronize configurations, DNS configuration, and persistence to provide stateful-failover of DNS query	Clause stands deleted

		FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 WAF			
97.	137	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 WAF	SL No. 406	Supports an GUI integrated zone file management tool that simplifies DNS zone file management and reduce the risk of misconfiguration. It shall provide a secure environment to manage DNS infrastructure while validating and error-checking zone files. It shall be built on the latest version of BIND.	**Should be supplied with inbox or centralized management-CLI, GUI for policy configuration and verification**
98.	137	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 WAF	SL No. 407	Supports DNS A, AAAA, A6, CNAME, DNAME, HINFO, KEY, MX, NS, NXT, PTR, SIG, SOA, SRV and TXR records	Supports DNS A, AAAA record
99.	138	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NDR	SL No. 427, Storage	Dual Hot swappable. Storage. 2 x 4TB, with SSD or min 7.2k RPM HDD	Dual Hot swappable Storage memory Capacity of atleast 2 x 4TB SSD or 7.2k RPM HDD. **Bidder has to factor storage as per the scope defined in the RFP by the Bank**
100.	138	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NDR	SL No. 428, Throughput	Inline Web Traffic Analysis -20 Gbps (rated HTTP throughput)	Throughput threat prevention - 20 Gbps (**rated multi-protocol throughput including** HTTP, **SMTP,SMB, FTP, RDP and other protocols**)
101.	138	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE	SL No. 429	Throughput Scalability (without any additional hardware) Inline Web Traffic Analysis -40 Gbps (rated HTTP throughput)	Throughput Scalability (without/**with any additional hardware)** Inline Web Traffic Analysis - atleast 40 Gbps **(rated HTTP throughput)(rated multi-protocol throughput including** HTTP**, SMTP,SMB, FTP, RDP and other protocols)**

		SOLUTION, Table 1 NDR			
102.	138	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NDR	SL No. 430	Form Factor 1RU(Preferably) in standard 42U Rack	Clause stands deleted
103.	138	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NDR	SL No. 431, Ports	8x10/25/40 GE copper or a mix of (4x 1 G copper and 4 x 10G SFP+ fiber) number of Interfaces having a separate dedicated management and IPMI port.	Minimum 8x10/25/40 GE **copper or fiber ports**
104.	138	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NDR	SL No. 432	Able to detect multiple infection vectors (Network, Email, Files) as a dedicated purpose-built platform deployed independently without any functional reliance on existing layers of security like NGFW, NGIPS, Proxy etc. adhering to defense in depth architecture, where, If any of the layers of core underlying security get replaced or non-functional, the proposed solution must be capable to function on its own.	Able to detect multiple infection vectors (Network, Files, **https, http**) as a dedicated purpose-built platform deployed independently without any functional reliance on existing layers of security like NGFW, NGIPS, Proxy etc. adhering to defense in depth architecture, where, If any of the layers of core underlying security get replaced or non-functional, the proposed solution must be capable to function on its own.
105.	138	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 WAF	Sl No. 423	OEM should be in the Gartner's and Forrester Leader's or challengers Quadrant report for Web Application Firewall as per the latest WAF report.	Clause stands deleted
106.	138	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 WAF	SL No. 424	The Solution should be ICSA certified with publicly available reference for WAF.	Clause stands deleted

107.	139	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NDR	SL No. 440	Support an inline blocking/monitoring mode preferably along with Inline Proxy, TAP/SPAN, ICAP etc. Out of Band TCP Reset should not be the only acceptable form of blocking	Support an inline monitoring or blocking mode preferably along with Inline Proxy, TAP/SPAN, ICAP etc. **or by using third party integration such as SOAR/API or any other means**
108.	139	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NDR	SL No. 441	Inline blocking mode that automatically blocks inbound exploits and malware and outbound multi-protocol callbacks.	Inline monitoring or blocking mode that automatically blocks inbound exploits and malware **by using third party integration such as SOAR/API or any other means or by using inbuilt capabilities**
109.	139	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NDR	SL No. 450	Capable of protection against advanced attacks and malware types that are difficult to detect via signatures like web shell uploads, existing web shells, ransomware, cryptominers etc.	Capable of protection against advanced attacks and malware types that are difficult to detect via signatures like web shell uploads, existing web shells, ransomware, cryptominers etc. **The preventive mechanism may be achieved through inbuilt or through integration with DDoS Solution, Firewalls, NIPS or other preventive devices proposed by bidder**
110.	139	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NDR	SL No. 451	Utilize multiple machine learning, AI and correlation engines represent a collection of contextual, dynamic rules engines that detects and blocks malicious activity in real-time and retroactively, based on the latest machine-, attacker- and victim- intelligence.	Utilize multiple machine learning, AI and correlation engines represent a collection of contextual, dynamic rules engines that detects and blocks malicious activity **by using third party soar/api/ or thorough internal mechanism** and retroactively, based on the latest machine-, attacker- and victim- intelligence.
111.	139	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NDR	SL No. 456	Detect malicious TLS connections using a combination of JA3 blacklists and other logic/models designed to detect malicious activity based on TLS session attributes	Detect malicious TLS connections using a combination **of available technologies**
112.	140	Annexure XI(A) TECHNICAL AND	SL No. 458	Proposed solution should be a standalone dedicated purpose built solution that must provide full Detection, Network Visibility, Investigation & Forensic capability,	Proposed solution should be a redundant dedicated purpose built solution that must provide full Detection, Network Visibility, Investigation & Forensic capability, through high speed lossless

		FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NDR		through high speed lossless packet capture & analysis functions for a network traffic capture for 20 Gbps. Network Traffic capture capacity >20 Gbps- 5 Marks(Max) else 1 Mark(Max)	packet capture & analysis functions for a network traffic capture for 20 Gbps. Separate setup to be deployed **for DC and DR** Network Traffic capture capacity >=20 Gbps- 5 Marks(Max) else 1 Mark(Max)
113.	140	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NDR	SL No. 465	Provide native Disk encryption capability to ensure captured raw packets are secured.	Provide encryption capability to ensure security of captured data packets
114.	140	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NDR	SL No. 472	Asymmetric flow analysis	Clause stands deleted
115.	140	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NDR	SL No. 475	Support capability to upload packet captures (PCAP's) captured outside the solution for analysis	Support capability to upload**/download** packet captures (PCAP's) outside the solution for analysis
116.	140	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NDR	SL No. 481	Provide an intelligent Capture functionality for selective filtering of captured traffic to eliminate streaming video, large file transfers, unwanted encrypted payloads, etc. to optimize storage	Provide an intelligent **policy driven flow capture to optimize storage**
117.	141	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIO	SL No. 482	Capable to have Real-time indexing of all captured packets using time stamp and connection attributes. Export of flow index and connection metadata in JSON format. Flow index must be converted to NetFlow v9, IPFIX and Silk Tools data formats	Capable to have Real -time indexing of all captured packets using time stamp and connection attributes

		NS OF THE SOLUTION, Table 1 NDR			
118.	141	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NDR	SL No. 483	Ability to capture network traffic and import packet capture files (pcap) using the same infrastructure	**OPTIONAL:** Solution should be able to capture network traffic and the data collected should be stored as PCAP or any other format for traffic analysis.
119.	141	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NDR	SL No. 484	Asymmetric flow analysis of individual or bulk PCAP data for sessions of interest	Clause stands deleted
120.	141	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NDR	SL No. 487	Solution must have a dedicated Malware Analysis engine with purpose built platform having windows, Linux and MAC O.S environments	Solution must have a dedicated **on premises** Malware Analysis engine with purpose built platform having windows, Linux and MAC O.S environments. **Bidder may size the system as per the best available option.**
121.	141	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NDR	SL No. 489	Capability to provide Back-in-time IOC threat analysis via integration of 3rd party Threat Intelligence, STIX, and OpenIOC feeds with automated Investigation and analysis search function.	Capability to provide Back-in-time IOC threat analysis via integration of 3rd party Threat Intelligence, STIX, and OpenIOC feeds with automated Investigation and analysis search function **or integration with its own Threat Intelligence.**
122.	141	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NDR	SL No. 490	The storage for raw packets should preferably be OEM provided SAS connected to ensure support, performance and compatibility is maintained. The data should directly be available to appliance for reporting and investigation at high read/write I/O speeds with performance guarantee as per publicly available datasheet	Clause stands deleted

123.	141	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NDR	SL No. 491	Web based GUI and a unified security dashboard displaying the real time consolidated data in graphical/textual format and all alerts received from and detected by web traffic, email and malware analysis systems deployed in centralized/decentralized architecture. The solution should have the ability to view and identify the infected systems and drill down into infection details at centralized location.	Web based GUI and a unified security dashboard displaying the real time consolidated data in graphical/textual format and all alerts received from and detected by all the traffic and malware analysis systems deployed in centralized/decentralized architecture. The solution should have the ability to view and identify the infected systems and drill down into infection details at centralized location.
124.	141	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NDR	SL No. 492	Store minimum 30(Thirty) 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.	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**
125.	141	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NDR	SL No. 496	Malware Analysis provides users with two analysis modes—live and sandbox. The solution should provide VNC and environment custom configuration to the sandbox VM's for the analysis of specific samples whenever required	Malware Analysis provides users with two analysis modes — live and sandbox. The solution should provide VNC or recorded reports as required by the Bank
126.	141	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NDR	SL No. 498	Solution should provide link to export the pcap or video files for further forensics that can be performed on the actual objects, particular file or URL and files created or modified during malware analysis.	Solution should facilitate export the pcap or video files for further forensics
127.	142	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NDR	SL No. 502	Dynamic Analysis must provide exhaustive data on analysis for Application Exceptions, API Calls, Command Injection, Code Injection, DLL-Loading, Doc summaries, exploit code, First Rapid Memory Operation, Heap Spraying, Hidden processes, java call, Mutex, Network activities, Process, Protection changes, registry keys, stack pivot, threads, WMI Queries etc. from object emulation and execution	Clause stands deleted
128.	142	Annexure XI(A) TECHNICAL AND	SL No. 503	Solution should provide a configuration for auto-remediating via Graph API's for retrospective detections in mailbox and appropriately remediation policy should be set to Retroactive	Clause stands deleted

		FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NDR		(Auto), Manual or Native modes, or all three. Remediation policies must provide Actions like Quarantine, Move, Permanent Delete, and Take No Action (Monitor) for a seamless Email Detection & response.	
129.	142	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NDR	SL No. 505	Solution must provide Quarantine-Digest Access to allows administrators to configure the network locations from which the end users can manage their quarantines.	Clause stands deleted
130.	142	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NDR	SL No. 506	The email threats must be analyzed with Machine learning and AI based engines for detecting Spear phishing advance threat campaigns.	Clause stands deleted
131.	142	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NDR	SL No. 508	Device should be a single standalone dedicated file analysis solution with agentless analysis engine to detect zero-day, advance APT attacks and other evasive attacks using dynamic, signature-less analysis in a safe, dynamic analysis environment for minimum 70000 unique file analysis per day on each appliance.	Device should be dedicated file analysis solution with agentless analysis engine to detect zero-day, advance APT attacks and other evasive attacks using dynamic, signature-less analysis.
132.	142	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NDR	SL No. 509	Support agentless scanning of storages using protocols like CIFS, WebDAV, sharepoint, and NFS-compatible file shares, without affecting performance of DAT servers. The option for scanning multiple mounted share locations for continuous analysis of all stored files including analysis of a wide range of file types is required.	**OPTIONAL:** Support agentless scanning of storages using protocols like CIFS, WebDAV, sharepoint, NFS-compatible file shares, etc, without affecting performance of DAT servers.
133.	142	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE	SL No. 512	The File APT Solution must provide ability to create a quarantine share folder and move malicious files to that share folder as well as the ability to move clean files to the designated clean share folder with built-in automated workflow.	Clause stands deleted

		SOLUTION, Table 1 NDR			
134.	143	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NDR	SL No. 518	Central Management must be supplied with minimum 2x 1GigE BaseT Network interfaces ports with a separate dedicated Management & IPMI ports, having minimum storage capacity of 4x 4 TB HDD, on RAID 10 with minimum usable storage of 8TB and redundant power supply.	Central Management must be supplied with minimum 2x 1GigE BaseT Network interfaces ports with a separate dedicated Management & IPMI ports, having minimum storage capacity of 4x 4 TB HDD, on RAID 10**/RAID5/RAID6** with minimum usable storage of 8TB and redundant power supply.
135.	143	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NDR	SL No. 521	Monitoring/prevention of Internet based traffic, Reporting and analytics should be in place for real-time monitoring of the egress and ingress traffic to understand 360 degree view.	Monitoring/prevention of Internet based traffic, Reporting and analytics should be in place for real-time monitoring of the egress and ingress traffic to understand 360-degree view. **Prevention by using third party integration such as SOAR/API or any other means or by using inbuilt capabilities**
136.	143	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NLB, GSLB External ADC	SL No. 534, Power on Demand	Dual AC/DC supply with hot swappable units, with always on management & LED to initial configuration	Dual AC/DC supply with hot swappable units
137.	143	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NLB, GSLB External ADC	SL No. 536, Ports	4X40GE QSFP+ SR4 , 8X10GE SFP+ ports & 4X100GE SFP+ Ports	(4X40GE QSFP+ SR4 **or 4X100GE SFP+ Ports)** and (8X10GE SFP+ ports) SFP+/QSFP+ **1X1G Management port** **All ports should be fully populated**
138.	144	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIO	Sl No. 545	The ADC should support auth enforcement prior to allowing access to HTTP/HTTPS SLB application - LDAP RADIUS, SAML, Oauth, Client certificate authentication, Web API Callout	**Optional:** The ADC should support auth enforcement prior to allowing access to HTTP/HTTPS SLB application - LDAP RADIUS, SAML, Oauth, Client certificate authentication, Web API Callout

		NS OF THE SOLUTION, Table 1 NLB, GSLB External ADC			
139.	146	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NLB, GSLB External ADC	Sl No. 588, Scoring	Appliance should be able to function as Authoritative Domain Name Server (ADNS), DNS proxy server / End Resolver / Forwarder and should be able to host SRV Records, AAAA Records, A Records, MX Records, NS Records, CNAME Records, PTR Records, SOA Records and should also support DNSSEC	Clause stands deleted
140.	144	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NLB, GSLB External ADC	Sl No. 549	L4 to L7 DDoS Protection against TCP/UDP/ICMP/DNS Flooding / Amplification, HTTP GET/POST Floods, Malformed SSL Floods, SSL Session Floods	Clause stands deleted
141.	144	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NLB, GSLB External ADC	SL No. 599	The ADC solution shall conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950	Clause stands deleted
142.	144	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NLB,	SL No. 600	The ADC solution shall conform to EN 55022 Class A/B or EN 55032 Class A/B or CISPR22 Class A/B or CISPR32 Class A/B or CE Class A/B or FCC Class A/B	Clause stands deleted

		GSLB External ADC			
143.	144	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NLB, GSLB External ADC	SL No. 602	Damping Sudden Surge in traffic so it does not overwhelm the servers by tracking the number of connections to the server, and adjust the rate of new connections to the server	Clause stands deleted
144.	144	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NLB, GSLB External ADC	Sl No. 588	Appliance should be able to function as Authoritative Domain Name Server (ADNS), DNS proxy server / End Resolver / Forwarder and should be able to host SRV Records, AAAA Records, A Records, MX Records, NS Records, CNAME Records, PTR Records, SOA Records and should also support DNSSEC	Clause stands deleted
145.	145	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NLB, GSLB External ADC	SL No. 562	The solution must have ICAP integration with other security devices for file vulnerability, virus, Trojan scanning during file submission with web-applications to improve security	The solution must have ICAP integration with other security devices for file vulnerability, virus, Trojan scanning during file submission with web-applications to improve security **or equivalent or built-in AV**
146.	145	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NLB, GSLB External ADC	Sl No. 565, 548, 601	DNS Security: GSLB Endpoints on the ADC should have safeguard against DNS DDoS attacks, random subdomain attacks, cache poisoning, cache bypass attacks, and should support enforcing DNS transactions over TCP	Clause stands deleted

147.	145	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NLB, GSLB External ADC	Sl No. 574	Supports an GUI integrated zone file management tool that simplifies DNS zone file management and reduce the risk of misconfiguration. It shall provide a secure environment to manage DNS infrastructure while validating and error-checking zone files. It shall be built on the latest version of BIND.	Solution should **have inbox or centralized management-CLI, GUI for policy configuration and verification**
148.	147	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 MFA	SL No. 608	Solution should be software token based and capable of generating synchronous token such as TOTP, etc . Bidder has to provide Applications on all Android (7 and above), IOS(10 and above) including their future versions. The application must be present on Playstore/ Appstore and have a robust, comfortable interface.	Solution should be software token based and capable of generating synchronous token such as TOTP **or HOTP**, etc . Bidder has to provide Applications on all Android (7 and above), IOS(10 and above) including their future versions. The application must be present on Playstore/ Appstore and have a robust, comfortable interface.
149.	147	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 MFA	SL No. 605	MFA should be hardware based and the solution including the software should be deployed on-premises	Proposed MFA solution should be hardware based or **software based with underlying hardware infra** and deployed on-premises
150.	147	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 MFA	SL No. 616	Should have Authentication at protocol level	Clause stands deleted
151.	147	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 MFA	SL No. 620	MFA should be able to integrate with third party applications such as reverse proxy solution and PIM solution	MFA solution should be able to integrate with any third-party application **that support Radius, LDAP, SAML 2.0 or OIDC as authentication protocols, third party applications hosted in Bank for internal users as well as for customers as per the banks requirement**

152.	148	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 MFA	SL No. 625	The proposed solution should have OATH compliant time based	The proposed solution should have **OAUTH** compliant time based
153.		Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 ADC	Anti DDoS Technical Specs, BOM, Commercial	Addition of New Clause	**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.**
154.		Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 Anti DDoS/DDoS Preventive Module		Addition of New Clause	**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.**
155.	Addition	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NDR		**CPU**	**Minimum 24 Core**
156.	Addition			**Storage**	**Minimum 2x 1TB U.2 Enterprise-class SSD (RAID 1 Mirrored)**
157.	Addition			**RAM**	**Minimum 256 GB**
158.	Addition			**Power on demand**	**Dual AC/DC supply with hot swappable units, with always on management & LED to initial configuration**

159.	Addition			**Form Factor**	**1RU/2RU in standard 42U Rack**
160.	Addition			**Ports**	**4*100G ports and 16*25G/10G with negotiable to 10G with SFP+/ QSFP+ as per the compatible interfaces**
161.	Addition			**SSL Inspection specifications**	**Device should feed decrypted traffic to security device in service chain for inspection received from end user and encrypt before sending it to back end application.**
162.	Addition				**should support encryption and decryption for TLS 1.3,1.2 and SSL traffic with ECC, RSA cipher support.**
163.	Addition				**Should support 200K SSL TPS of 2048 key size. Device should support both L2 and L3 deployment with ICAP support**
164.	Addition				**device should provide ADC functionality as mentioned in RFP and should support virtualization.**
165.	Addition				**L7 throughput of device should be minimum 180 Gbps**
166.	Addition				**Solution should provide all functionality on single OS instance and hardware and software should be from same OEM**
167.	Addition				**Solution should able to categories internet outbound traffic including office 365.**
168.	143	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION, Table 1 NLB, GSLB External ADC	529	24 Core	**24 Physical Cores**

ANNEXURE-XI(A)
TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION (REVISED)

S.N.	Mandatory Functional/ Technical Requirements		Mandatory/ Weightage	Max Score	Compliance (Yes/No)	Remarks/ Specification on Proposed Device	Score Obtained
Internet Router							
Minimum Core Specifications: 11 Marks							
1.	**Throughput**	IP Sec: 80 Gbps or higher Total System bandwidth: 120 Gbps	Mandatory	1(Max)			
2.	**Throughput Scalability**	IP Sec:100 Gbps or higher Total System bandwidth: 150 Gbps	Mandatory	1(Max)			
3.	**Power on demand**	Atleast 2 Redundant AC/DC power supply	Mandatory	1(Max)			
4.	**Ports**	12x1/10GE WAN ports, 2X40GE and 2X40/100GE SPF/SPF+ base ports	Mandatory	1(Max)			
5.	**Line Cards**	2 line cards with 10,40,100 Gigabit Ethernet ports	Mandatory	1(Max)			
6.	**RAM**	16GB and upgradable to 32 GB	Mandatory	1(Max)			
7.	**Form Factor**	1U(Preferably) in standard 42U Rack	Weightage	1U -2 Marks (Max) 2U -1 Mark Others-0 Mark			
8.	**Protocols**	IPv4, 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+.	Mandatory	1(Max)			
9.	**Encapsulations**	GRE, Ethernet, 802.1q VLAN, PPP, HDLC, PPPoE	Mandatory	1(Max)			
10.	**Encryptions/ Authentication**	DES, 3DES, AES-128, AES-256, MD5, MD5, SHA, SHA-256, SHA-384, SHA-512	Mandatory	1(Max)			
Others Features: 15 Marks							
11.	Support for QoS		Mandatory	1(Max)			

12.	Supported IPv4 and IPv6 routes: 4M each		Mandatory	IPv4 and IPv6 routes more than 5M from Day 1- 5 Marks(Max) else 1 Mark			
13.	Device should have High Availability(Both Active-Active and Active Passive)		Mandatory	1(Max)			
14.	Supports SDWAN with IPSec Throughput – 30 Gbps		Weightage	Yes-5 Marks(Max) No-1 Mark			
15.	Support for atleast 3000 ACLs		Mandatory	3000 ACLs- 1 Mark 3000-4000 ACLs-2 Marks 4000+ACLs- 3 Marks			
Total Marks				**26(Max)**			
Interconnect Switches							
Minimum Core Specifications: 8 Marks							
16.	**Forwarding rate**	1400 Gbps+	Mandatory	1(Max)			
17.	**Switching fabric**	2000 Gbps+	Mandatory	1(Max)			
18.	**Power**	Hot swappable redundant power supply	Mandatory	1(Max)			
19.	**Ports**	24/48 nos. 25G/40G SFP/SFP+/QSFP based ports with 100G SFP/SFP+/QSFP+ based uplink Ports	Mandatory	1(Max)			
20.	**RAM**	16GB	Mandatory	1(Max)			
21.	**Form Factor**	1U(Preferably) in standard 42U Rack with stacking	Weightage	1U -2 Marks(Max) 2U -1 Mark Others-0 Mark			
22.	**Protocols**	IPv4, IPv6, static routing, RIP, PIM, OSPF, VRRP, PBR, QoS, BGPv4, BGPv6 , MPLS, VRF, VXLAN, IS-ISv4, OSPFv3, MP-BGP, SSHv2, SNMPv2c, SNMPv3, NTP, RADIUS, TACACS+.	Mandatory	1(Max)			
Others Features: 22 Marks							
23.	Support for QoS		Weightage	Yes-5 (Max) No-0 Mark			
24.	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.		Mandatory	1(Max)			

25.	IPv6 Binding Integrity Guard, IPv6 Snooping, IPv6 RA Guard, IPv6 DHCP Guard, IPv6 Neighbour Discovery Inspection and IPv6 Source Guard.		Mandatory	1(Max)			
26.	Multimode SPF module for all ports		Weightage	Yes-5 Marks(Max) No-0 Marks			
27.	Support 32K MAC addresses, 16K IPv6 and 32K IPv4 routes, 1000 active VLANs		Mandatory	1(Max)			
28.	Switch should have minimum 2000Gbps of switching fabric and 1488 Mbps of forwarding rate. Should support minimum 32K MAC Addresses and 1000 active VLAN ; Should Support minimum 32K IPv4 routes or more and 16K IPv6 routes or more		Mandatory	1(Max)			
29.	Redundant hot-swappable fans		Mandatory	1(Max)			
30.	Active-Active / Active-Passive High Availability		Mandatory	1(Max)			
31.	HA Active-Active/Active-Passive with Clustering		Weightage	Yes-5 Marks(Max) No-0 Marks			
32.	IPv4 and IPv6 ACL		Mandatory	1(Max)			
Total Marks				**30(Max)**			
Anti DoS/ DDoS preventive module							
Minimum Core Specifications: 8 Marks							
33.	Throughput	Inspection and Mitigation: 20 Gbps DDoS Flood Attack Prevention Rate: Minimum 30 Mpps DDoS Cloud Mitigation: 4 Gbps	Mandatory	1(Max)			
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	Mandatory	1(Max)			
35.	Power on demand	Redundant 2 AC/DC power supplies	Mandatory	1(Max)			
36.	RAM	32 GB	Mandatory	1(Max)			

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	Mandatory	1(Max)			
38.	Latency	<=80 microseconds	Mandatory	1(Max)			
39.	Form Factor	1U/2U (preferably) in standard 42U Rack	Weightage	1U/2U -2 Mark(Max) Others-0 Marks			
Other Features: 93 Marks							
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.	Mandatory	5 Analysts- 2 Marks 6-7 Analysts-3 Marks More than 7 Analysts- 5 Marks			
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.	Mandatory	1(Max)			
42.	Proposed product/solution should be stateless Technology not having any kind of state limitation e.g. TCP connections.	Mandatory	1(Max)			
43.	Detect and Mitigate both inbound and outbound traffic	Mandatory	1(Max)			
44.	Work in fail open or fail close mode in all the ports or should support software bypass capability or should be achieved through additional external switch populated with same interfaces capacity	Mandatory	1(Max)			
45.	Protect from multiple attack vectors on different layers at the same time with combination OS, Network, Application, and Server side attacks	Mandatory	1(Max)			
46.	Detect and mitigate IPV4 & IPv6 Attacks	Mandatory	1(Max)			

47.	Detect and block the traffic originated from any specific using Geo location based filtering (IPV6 AND IPV4).	Mandatory	1(Max)			
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)The solution has Inbuilt mechanism to inspect traffic with external threat intelligence feed and shall support at least 3Million hash for inline blocking	Mandatory	Both a & b - 5 Marks (Max) Only a - 2 Marks			
49.	Detect and block traffic originated from source IP address(IPV6 AND IPV4) from TOR network	Weightage	Yes- 10 Marks(Max) No-0 Marks			
50.	Support Symmetric and Asymmetric Traffic flows	Mandatory	1(Max)			
51.	Support integration of external Threat Intelligence Platform (TIP) and Support Threat Intelligence Feed	Mandatory	1(Max)			
52.	Detect and block ICMP, DNS Floods, FTP Floods, Botnets	Mandatory	1(Max)			
53.	Detect and Mitigate attacks at Layer 3 to Layer 7	Mandatory	1(Max)			
54.	Protect from TCP Out-Of-State attacks	Mandatory	1(Max)			
55.	Transparent bridge to pass 802.Q tagged frames and other control protocols VLAN, L2TP and GRE traffic.	Mandatory	1(Max)			
56.	Detect misuse of application protocols in the network like HTTP/POP3/STP/SIP/SMTP/FTP	Mandatory	1(Max)			
57.	Mitigation mechanism to protecting against zero-day DoS and DDoS attacks without manual intervention	Mandatory	1(Max)			
58.	Protect against SSL/TLS-encrypted DoS and DDoS threats both at the SSL /TLS layer and HTTPS layer System should Protect against SSL/TLS-encrypted Attacks	Mandatory	1(Max)			
59.	Block invalid packets (including checks for Malformed IP Header, Incomplete Fragment, Bad IP Checksum, Duplicate Fragment, Fragment Too Long, Short Packet, Short TCP Packet, Short UDP Packet, Short ICMP Packet, Bad TCP / UDP Checksum, Invalid TCP Flags, Invalid ACK Number) and provide statistics for the packets dropped. Solution should also support packet Anomaly Protection	Mandatory	1(Max)			
60.	Support deployment on a "logical link bundle" interfaces, In-Line, Out-of-Path deployments modes.	Mandatory	1(Max)			
61.	Learning mode to easily identify anomalies in the network communication.	Mandatory	1(Max)			
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	Mandatory	Supports CAPTCHA- 5 Marks (Max) Supports HTTP – 2 Marks			

63.	Detect and protect from unknown Network & application layer DDOS attacks and should not have dependency on signatures for such attacks. System should support Behavioural based predictive DDoS protection	Mandatory	1(Max)			
64.	Support suspension/dynamic suspension of traffic from offending source based on a signature detection and attack countermeasures	Mandatory	1(Max)			
65.	Support minimum 90,000 SSL CPS RSA 2048-bit key strength (Should have Built in SSL card). Also System should have ability to scale SSL CPS capacity via external SSL appliance retaining proposed DDoS appliance (CPS: Connections Per Second)	Mandatory	1(Max)			
66.	Support the dropping of idle TCP sessions if client does not send a user-configurable amount of data within a configurable initial time period and should dynamically blacklist the offending sources	Mandatory	1(Max)			
67.	Allow Network Security policies to be changed while the policy is in active blocking mode and should not affect running network protection.	Mandatory	1(Max)			
68.	Should have countermeasures & challenge response based approach for immediate mitigation of flood attacks—protecting against unknown DDoS attacks without manual intervention. The system should not depend on only signatures for mitigation of DDOS attacks.	Mandatory	1(Max)			
69.	Able to detect and block SYN Flood attacks and should support different mechanism a) SYN Protection - TCP Authentication b) SYN Protection - Out of Sequence Authentication c) SYN Protection - TCP Reset	Mandatory	1(Max)			
70.	Able to detect and block HTTP GET Flood and should support following mechanism to avoid False Positive prevention (or equivalent): a)TCP Authentication b) HTTP Redirect c) JavaScript redirect	Mandatory	1(Max)			
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	Mandatory	1(Max)			
72.	Protect from Brute Force/reflection & amplification attacks or equivalent	Mandatory	1(Max)			
73.	Detect from Known DDoS attack Tools without any performance impact	Mandatory	1(Max)			
74.	Support configuration via standard up to date web browsers	Mandatory	1(Max)			
75.	Support for scalable SSL TPS capacity, either internally or via integration of external appliance (TPS: Transactions Per Second)	Mandatory	1(Max)			
76.	Provide protection for known attack tools that attack vulnerabilities in the SSL layer itself or separate SSL offloading device	Mandatory	1(Max)			
77.	support following environments: Symmetric, Asymmetric Ingress, Asymmetric Mesh	Mandatory	1(Max)			
78.	Support horizontal and vertical port scanning Behavioural protection	Mandatory	1(Max)			
79.	Built-in hardware bypass or software bypass for all interface types	Mandatory	1(Max)			

80.	Detect and Mitigate different categories of Network Attacks viz viz. Volume based, Protocol, Application attacks etc.	Mandatory	1(Max)			
81.	Should detect SSL encrypted attacks at Key size 1K & 2K without any hardware changes.	Mandatory	1(Max)			
82.	Able to detect and protect from Zero-Day Network DDoS/DDoS flood attacks on the basis of behavioural DDoS attacks/challenge response mechanism or by an automatically created signature within a minute and must be mentioned in data sheet	Weightage	Yes- 10 Marks(Max) No-0 Marks			
83.	Identify malicious SSL traffic based on behavior analysis and to decrypt only malicious identified traffic instead of inspecting entire traffic to reduce the latency.	Mandatory	1(Max)			
84.	Cloud signalling to signal to upstream ISPs or managed service provider who is providing anti-DDoS cloud service for very large DDoS attack mitigation.	Mandatory	1(Max)			
85.	DDoS Appliance must not have any limitations in handling the number of concurrent session for DDoS attack traffic - Knowing nature of solution and should be clearly mentioned in public facing datasheet.	Mandatory	1(Max)			
86.	Device should have High performance architecture to ensure that attack mitigation does not affect normal traffic processing.	Mandatory	1(Max)			
87.	Quoted OEM should have Global Technical Assistance (TAC) support in India	Mandatory	1(Max)			
88.	Support option for Centralized management of multiple devices.	Mandatory	1(Max)			
89.	Support Role/User Based Access Control and reporting functionality.	Mandatory	1(Max)			
90.	System should have mechanism to upgrade the firmware and application	Mandatory	1(Max)			
91.	In inline mode system must not modify MAC or IP addresses of passed frames	Mandatory	1(Max)			
92.	The Device must have an updated IP reputation feed that describes suspicious traffic Blacklisted IPs, botnets, Phishing. It should be updated atleast once hourly to block and protect network against active attackers. Same may be facilitated integrate with its proprietary Threat intelligence or may take feed from reputed Threat intelligence experts which can provide compliance to points mentioned sub paras (the commercial for external /internal threat intelligence feed should be factored in commercial section for 5 years)	Mandatory	1(Max)			
93.	Should support user customizable/ user definable signature/countermeasures	Mandatory	1(Max)			
94.	System should be able to provide Challenge action apply to suspicious/all source.	Mandatory	1(Max)			
95.	System DNS protection should employ challenge/response mechanism	Mandatory	1(Max)			
96.	Real-time events correlation between Multi Vector Attacks viz. Volume based, Protocol, Application attacks etc.	Mandatory	1(Max)			

97.	Device should integrate with Banks existing SIEM engine seamlessly through syslog messages		Mandatory	1(Max)			
98.	System should accurately follow attack vector changes without pcap analysis required or manual scripts		Mandatory	1(Max)			
99.	Solution should provide comprehensive countermeasure for DNS protection including random sub-domain based attacks like DNS water torture attacks		Mandatory	1(Max)			
100.	System should have out-of-path / on device SSL inspection		Mandatory	1(Max)			
101.	System protects against SSL/TLS-encrypted DoS and DDoS threats in incoming and outgoing traffic		Mandatory	1(Max)			
102.	All components of the solution should be capable of both Active-Active and Active Passive High Availability and the feature should be enabled from Day 1		Mandatory	1(Max)			
DDoS Cloud Mitigation: 5 Marks							
103.	Protection from all attacks like UDP Flooding, ICMP Flooding, Spoofed packet Flooding,SYN Floods, fragmented packet attacks, Ping od Death, Smurf, GET/POST floods,slow-and-slow attacks, Zero Day DDoS. Open BSD vulnerabilities etc.		Mandatory	1(Max)			
104.	Bandwidth should be dedicated and not shared. Connectivity required, if any, will have to be arranged and factored by the bidder.		Mandatory	1(Max)			
105.	OEM should provide 24X7 Single Point of Contact(SPOC) details for any issue.		Mandatory	1(Max)			
106.	Service should be always on		Mandatory	1(Max)			
107.	Should support features like null routing, sinkholing, scrubbing, IP masking, Application layer mitigation, DNS name server protection, application protection with uptime SLA of 99.99%		Mandatory	1(Max)			
Total Marks				**106 Marks(Max)**			
Network Intrusion Prevention System (NIPS)							
Minimum Core Specifications: 10 Marks							
108.	Throughput	System:20 Gbps (with all features enabled)with mix traffic inspection	Mandatory	Inbuilt SSL Inspection 10 Gbps- 6 Marks (Max), Inbuilt SSL Inspection 7 Gbps- 3 Marks, Inbuilt SSL Inspection <7 Gbps- 1 Mark			
109.	Throughput Scalability	System: 30 Gbps (with all features enabled)	Mandatory	1(Max)			

110.	Power on demand	Redundant 2 AC/DC power supplies	Mandatory	1(Max)			
111.	Ports	Minimum of 4X10G copper ports with fail open and 6 X40G QSFP+ fiber ports with fail open Dedicated 1 (1G / 100M) port for management console	Mandatory	1(Max)			
112.	Form Factor	1U/2U in standard 42U Rack	Weightage	1U/2U – 1 Mark(Max) Others - 0 Mark			
Others Features: 72 Marks							
113.	The solution should support on the box SSL inspection for inline as well as outbound traffic without dropping throughput capacity.		Mandatory	1(Max)			
114.	NIPS should support different mode of deployment. • IDS • TAP Mode • Inline • Simulation(Optional)		Weightage	Supports All 4 modes -5 Marks(Max) Doesn't support Simulation-2 Marks			
115.	Solution must accurately detect intrusion attempts and discerns between the various types and risk levels including Zero-Day attacks, unauthorized access attempts, pre-attack probes, suspicious activity, DoS, DDoS, vulnerability exploitation, brute force, hybrids. The NIPS solution should be able to perform deep inspection of network traffic by using a combination of advanced technologies, including full protocol analysis, threat reputation and behaviour analysis to detect and protect against Zero-day attacks, malware callbacks (C&Cs), Denial of service (DoS) and other advanced threats.		Mandatory	1(Max)			
116.	The Device/Appliance should support/have:						
a)	• Built-in SSL decryption Engine for SSL Traffic decryption to support prevention of encrypted attacks - which includes attacks over secured HTTP channel without need to have additional appliances.		Mandatory	1(Max)			
b)	• Outbound traffic SSL inspection.		Mandatory	1(Max)			
c)	• Anti-malware protection through various engines as part of solution offerings.		Mandatory	1(Max)			
d)	• Real time emulation techniques for embedded malware protection.		Mandatory	1(Max)			
e)	• Advanced DoS detection with "self-learning" for more accurate and fewer false positives.		Mandatory	1(Max)			
f)	• IPv4 and Ipv6 from day-one and detect attacks inside IPv6 encapsulated packets		Mandatory	1(Max)			
g)	• Protection from evasion based attacks		Mandatory	1(Max)			
h)	• Anti-spoofing capabilities		Mandatory	1(Max)			
i)	• Capability for Host quarantine and rate limiting		Mandatory	1(Max)			

117.	High availability in Active-active and active-passive mode with stateful failover and not only limited to transparent mode.	Mandatory	1(Max)			
118.	Protocol tunnelling for following:- IPv6, V4-in-V4, V4-in-V6, V6-in-V4, and V6-in-V6 tunnels, MPLS GRE Q-in-Q Double VLAN	Mandatory	1(Max)			
119.	Advanced botnet protection using following detection methods:- DNS/DGA, Fast flux, callback detection, DNS sinkholing, Heuristic bot detection ,Multiple attack correlation Command and control database	Mandatory	1(Max)			
120.	Control traffic based on geographical locations -- For e.g. a policy can be created to block traffic coming or going to a particular country. Provision should be there to allow specific IPs for any blocked country	Mandatory	1(Max)			
121.	Create Black List rules and White List rules which should allow to block or allow traffic to or from specified networks, based on protocols, applications, and other criteria.	Mandatory	1(Max)			
122.	Prioritize risk of threats to you with Campaigns detected and IP addresses that could be exposed	Weightage	Yes-5(Max) No-0			
123.	Quarantine user endpoint machine if it is communicating with bad vectors	Mandatory	1(Max)			
124.	Provide detailed host machine context at central dashboard	Mandatory	1(Max)			
125.	Inbound SSL Inspection detection and prevention using ECDHA or ECDHE cypher suits	Mandatory	1(Max)			
126.	Capability to provide outbound SSL inspection.	Weightage	Yes-5(Max) No-0			
127.	Multiple signatureless engines on the appliance without degrading the performance.	Mandatory	1(Max)			
128.	Dedicated emulation engine to provide protection from advanced attacks.	Mandatory	1(Max)			
129.	On-demand throughput scalability by just upgrading software license-Scalable on demand throughput based scalability without changing the hardware	Weightage	Yes-5(Max) No-0			
130.	Support Advanced Analytics, Heuristics and Machine Learning	Mandatory	1(Max)			
131.	Inbuilt network behavioural analysis engine to provide additional context using network flows.	Weightage	1(Max)			
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	Mandatory	1(Max)			
133.	Perform entire packet capture of the traffic and sent to the manager for analysis	Mandatory	1(Max)			
134.	Central management console	Weightage	Yes- 5 Marks (Max) No- 0 Marks			

135.	Management platform supports policy configuration, command, control, and event management functions for the NIPS appliances		Mandatory	1(Max)			
136.	Management console should support Radius and LDAP authentication in addition to the local user authentication		Mandatory	1(Max)			
137.	Management console should have the ability to allow access to specific hosts/users by enabling GUI Access and defining the list of authorized hosts/users		Mandatory	1(Max)			
138.	NIPS Management console should support high availability which should have Automated failover and fail-back		Mandatory	1(Max)			
139.	NIPS solution should provide Intelligent security management:- ■ Intelligent alert correlation and prioritization ■ Robust malware investigation dashboards ■ Preconfigured investigation workflows ■ Scalable web-based management		Mandatory	1(Max)			
140.	NIPS Management console should be capable of producing extensive graphics metric for analysis. Further, users should be able to drill down into these graphical reports to view pertinent details.		Mandatory	1(Max)			
141.	Dashboard details : CPU, memory, process utilization by device		Weightage	Yes-5(Max) No-0			
142.	Single point of contact from OEM for customer management, escalation backed by senior product specialists throughout the contract period.		Weightage	Yes-5(Max) No-0			
143.	OEM provides Schedules and performs Quarterly on-site visits; completes Protection Analysis and offers best practices recommendations. Such visits without any additional cost to the Bank.		Weightage	Yes-5(Max) No-0			
144.	Offered solution should have zero day, signature based prevention also inbuilt TLS decryptor		Mandatory	1(Max)			
Total Marks				**82 Marks (Max)**			
Next Generation Firewall with application monitoring capability (Antivirus blade, SSL/ TLS decryptor, Application control, URL filtering licenses to cater 0365 requirement, 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							
Minimum Core Specifications: 37 Marks							
145.	CPU	48 Physical Cores	Mandatory	1(Max)			
146.	RAM	256 GB	Mandatory	1(Max)			
147.	Storage	Minimum 400 GB SSD for system and 2 TB SSD for Logging capability	Mandatory	Storage Capacity 200% or more than proposed minimum – 3 Marks(Max) Else 1 Mark			

148.	Throughput	Inspection throughput- 30 Gbps IPsec VPN - 15 Gbps(AES256-SHA256) New Sessions-615,000 per second Concurrent Sessions -20M	Mandatory	1(Max)			
149.	Throughput Scalability	Inspection throughput- 100 Gbps IPsec VPN - 30 Gbps(AES256-SHA256) Sessions- 1,000,000 per second Concurrent Sessions -50M	Mandatory	Inspection Throughput 150 Gbps or more - 10 Marks (Max) Else 5 Marks			
150.	Power on demand	Redundant hot swappable fan and AC/DC power supplies	Mandatory	1(Max)			
151.	Tunnels protocol	SSL, IPSec, and XAUTH, Gateway-to-Gateway IPsec VPN Tunnels & Client-to-Gateway IPsec VPN Tunnels	Mandatory	1(Max)			
152.	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	Mandatory	2X100G -5 Marks(Max) 2X40G-2 Marks			
153.	Firewall policies	Atleast 50,000	Mandatory	200% of proposed minimum -3 Marks(Max) Else 1 Mark			
154.	VPN	14000 SSL VPN agent based remote VPN connection 200 site-to-site VPN	Mandatory	1(Max)			
155.	VPN Scalability	25000 SSL VPN agent based remote VPN connection 1000 site-to-site VPN	Mandatory	30,000+ SSL VPN- 5 Marks(Max) Else 1 Mark			
156.	Form Factor	Within 5U(Preferably) in standard 42U Rack	Weightage	5U or less -2 Marks (Max) Others-0 Mark			
157.	Protocols	Static, RIP v2, OSPFv2/v3 , BGP v4. The Next Generation Firewall must support DDNS including integration with third party DNS service providers : Mobile protocols : GTP, SCTP, etc. and support for termination of GRE Tunnels 1000 VLANs	Mandatory	1(Max)			

158.	Integrated functions	Firewall, IPSEC VPN, Application Awareness, IPS, BOT prevention, Antivirus, URL Filtering and Zero Day Threat Prevention.	Mandatory	1(Max)			
159.	Virtual Domains/ Virtual Instances/ Virtual systems/ etc.	Minimum 20	Mandatory	1(Max)			
Others Features: 16 Marks							
160.	Bidders are free to propose the asked functionality using one or at the maximum two devices.		Weightage	1 Device -5 Marks (Max) 2 Device -2 Marks			
161.	Proposed solution should offer chassis based modular architecture and must provide throughput scalability without changing the hardware/chassis i.e. the throughput scalability functionality is expected by Bank is with addition of processing modules only and should not be based on stacking units in clustering.		Mandatory	1(Max)			
162.	OEM provides single point of contact for customer management, escalation backed by senior product specialists throughout the contract period.		Weightage	Yes-2(Max) No-0			
163.	NGFW gateway architecture should have Control Plane separated from the Data Plane, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc.) & Network Processing (like flow control, route lookup, MAC lookup, QoS, NAT etc.).		Mandatory	1(Max)			
164.	Dashboard view and reporting of CPU usage (including real-time graph) for management activities and data plane CPU for other activities.		Mandatory	1(Max)			

165.	**Mandatory:** 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	Mandatory	Supports Optional Feature along with mandatory features - 5 Marks(Max) Supports only mandatory feature – 2 Marks			
166.	Support for both Client as well client less VPN. Must support Split tunnelling 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.	Mandatory	1(Max)			
Interface Operation Mode: 22 Marks						
167.	Support Active/Active and Active/Passive deployment mode and should support session state synchronization among Next Generation Firewalls in a high availability.	Mandatory	1(Max)			
168.	Support Dual Stack IPv4 / IPv6 application control and threat inspection support in: transparent mode (IPS Mode), Layer 2, Layer 3, Should be able operate mix of multiple modes	Mandatory	1(Max)			
169.	Support Ethernet Bonding functionality for Full Mesh deployment architecture.	Mandatory	1(Max)			
170.	Support & implement Zones, IP address, Port numbers, User id, Application id and threat protection profile under the same Next Generation Firewall rule or the policy configuration.	Mandatory	1(Max)			
171.	Native network traffic classification which identifies applications across all ports irrespective of port/protocol/evasive tactics.	Mandatory	1(Max)			
172.	Ability to create custom application signatures and categories directly on Next Generation Firewall without the need of any third-party tool or technical support. Also the device should have capability to provide detailed information about dependent applications to securely enable an application	Mandatory	1(Max)			
173.	Handle (alert, block or allow) unknown/unidentified applications like unknown UDP & TCP	Mandatory	1(Max)			
174.	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	Weightage	Yes-5 Marks(Max) No-0			
175.	Able to protect the user from the malicious content upload or download by any application. Example Blocking a malicious file download via a chat or file sharing application.	Mandatory	1(Max)			

176.	Support creation of policy based on wildcard addresses to match multiple objects for ease of deployment	Mandatory	1(Max)			
177.	Delineate different parts of the application such as allowing Facebook chat but blocking its file-transfer capability inside the chat application base on the content.	Mandatory	1(Max)			
178.	Inbuilt Automatic policy optimization to identify port-protocol based polices and convert the same into true application based polices. For example-Next Generation Firewall is configured with Security policy to allow port 80/443 and multiple applications (Facebook/ Rapidshare etc.) traffic going through the same policy, then the Next Generation Firewall should automatically identify those risky applications and help to add more application specific security policies which might be using the same ports (80/443). This will help Bank to tighten the application flow control and reduce the attack surface area.	Mandatory	1(Max)			
179.	Ability to manage Next Generation Firewall security policy even if management server is unavailable	Mandatory	1(Max)			
180.	Disallow root access to Next Generation Firewall system all users (including super users) at all times.	Weightage	Yes-2 Marks(Max) No-0			
181.	Support insertion of customer 2 Factor Authentication into any application before permitting the connection	Mandatory	1(Max)			
182.	Capability to create DOS prevention policy to prevent against DOS attacks on per zone basis (outbound to inbound, inbound to inbound and inbound to outbound) and ability to create and define DOS policy based on attacks like UDP Flood, ICMP Flood, SYN Flood (Random Early Drop and SYN cookie), IP Address Sweeps, IP Address Spoofs, port scan, Ping of Death, Teardrop attacks, unknown protocol protection etc.	Mandatory	1(Max)			
183.	All the proposed threat functions like IPS/vulnerability protection, Antivirus, C&C protection etc. should work in isolated air gapped environment without any need to connect with Internet.	Mandatory	1(Max)			
Threat Protection: 48 Marks						
184.	The NGFW should block the traffic based on Geo location (country wise).The Geo location-based configuration should be supported granularly for per policy and per application wise as per the business requirement.	Mandatory	1(Max)			
185.	Should have protocol decoder-based analysis which can statefully decodes the protocol and then intelligently applies signatures to detect network and application exploits	Mandatory	1(Max)			
186.	Intrusion prevention signatures should be built based on the vulnerability itself, A single signature should stop multiple exploit attempts on a known system or application vulnerability.	Mandatory	1(Max)			

187.	IPS must have options to create profiles for either client or server based protections, or a combination of both.	Weightage	Yes-2 Marks(Max) No-0			
188.	Integrated IPS capabilities with minimum 10000+ signature database. It should support importing signatures from third party tools, customizing IPS signature and creation of multiple IPS policy for different segments and zones.	Mandatory	Supports : 20,000 or more signatures - 10 Marks(Max), 15,000 to 19,999 signatures - 5 marks, Less than 15,000 signatures - 1 Mark			
189.	Solution should support payload-based signatures detect command-and-control (C2) traffic and are automatically-generated. This is to detect C2 traffic even when the C2 host is unknown or changes rapidly.	Weightage	Yes-5 Marks(Max) No-0			
190.	Perform content based signature matching beyond the traditional hash base signatures	Mandatory	1(Max)			
191.	On-box Anti-Virus/Malware, Anti Spyware signatures and should have latest updates of definitions throughout the contract period.	Weightage	Yes-5 Marks(Max) No-1			
192.	All the protection signatures should be created by vendor base on their threat intelligence and should not use any 3rd party IPS	Weightage	Yes-5 Marks(Max) No-0			
193.	Perform Anti-virus scans for HTTP, smtp, imap, pop3, ftp, SMB traffic with configurable AV action such as allow, deny, alert etc.	Mandatory	1(Max)			
194.	Define AV scanning on per application basis such that certain applications may be excluded from AV scan while some applications to be always scanned	Mandatory	1(Max)			
195.	Should block known network and application-layer vulnerability exploits	Mandatory	1(Max)			
196.	OEM should deliver new signatures for unknown attacks seen anywhere else in real-time as soon as new verdicts are available. This gives Bank almost instant access to OEM complete global intelligence data that is collected from a various sources that provides additional leverage for preventing successful attacks by minimizing Bank's exposure time to malicious activity.	Mandatory	1(Max)			
197.	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.	Mandatory	1(Max)			

198.	Should be able to call 3rd party threat intelligence data on malicious IPs, URLs and Domains to the Firewall policy in order to block those malicious attributes and such list should get updated dynamically with latest data	Mandatory	1(Max)			
199.	Solution should have event correlation across all logs and real-time i.e. anomaly detection, with Indicator of Compromise (IOC) and threat detection to reduce time-to-detect. The Indicators of Compromise (IOC) must identifies suspicious usage and artifacts observed on a network or in an operations system, determined with high confidence to detect intrusion.	Mandatory	1(Max)			
200.	The device should support zero day prevention by submitting the executable files and getting the verdict back in five minutes post detection.	Mandatory	1(Max)			
201.	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	Weightage	Yes-5 Marks(Max) No-0			
202.	Collect information about the security status of endpoints to take decision whether to allow or deny access to a specific host based on adherence to the host policies defined by organization before connecting to VPN.	Mandatory	1(Max)			
203.	Add custom threat prevention signature in an automated way by converting Snort or Suricata signatures into custom threat signatures.	Mandatory	1(Max)			
204.	Block malware, Phishing, proxy avoidance and other URLs by categories	Mandatory	1(Max)			
205.	Support HTTP/2 inspection	Mandatory	1(Max)			
DNS based attack Prevention: 11 Marks						
206.	Enable granular security to ensure that the remote host accessing the network resources are adequately maintained and adhere with defined security parameters before they are allowed access like minimum version of anti-virus software installed etc.	Mandatory	1(Max)			
207.	Maintain a database containing a list of known botnet command and control (C&C) addresses which should be updated dynamically. This should not be based on a static database.	Mandatory	1(Max)			
208.	Integrate and correlate to provide effective prevention against New C2 domains, file download source domains, and domains in malicious email links.	Mandatory	1(Max)			
209.	DNS Security should have predictive analytics to disrupt attacks that use DNS for Data theft and Command and Control.	Mandatory	1(Max)			
210.	DNS security should block known Bad domains and predict with advanced technology like machine learning	Mandatory	1(Max)			

211.	Specific DNS Security Signature Categories of domains based on the risk that these domains pose to Bank. Bank should be able to block DNS based attacks for include C2 (encompasses DGA and DNS tunnelling), malware, DDNS, newly registered domains, phishing, Dynamic DNS Domains, Domain Generation Algorithms and Newly Registered Domains. If such controls are not natively part of NGFW solution then bidder must propose an integrated platform solution to match the capabilities.	Mandatory	1(Max)			
212.	Capability to neutralize and block DNS tunnelling attacks.	Mandatory	1(Max)			
213.	Should have simple policy formation for dynamic action to block domain generation algorithms or sinkhole DNS queries.	Mandatory	1(Max)			
214.	Prevent against DNS tunnelling which are used by hackers to hide data theft in standard DNS traffic by providing features like DNS tunnel inspection	Mandatory	1(Max)			
215.	The Solution should support DNS security in line mode and not proxy mode.	Mandatory	1(Max)			
216.	The solution should have dynamic response to find infected machines and respond immediately. There should be provision for administrator to automate the process of sinkholing malicious domains to cut off Command and control and quickly identify infected users.	Mandatory	1(Max)			
Advanced Persistent Threat (APT) Protection: 33 Marks						
217.	APT Protection should be On-prem	Mandatory	1(Max)			
218.	Solution must have automated correlation engine on the appliance and on centralized management tool both which can correlate a series of related threat events that, when combined, indicate a likely compromised host on Bank's network	Mandatory	1(Max)			
219.	There should be provision to enable the APT solution from day-1 with following features: This should be a both on premise and OEM data lake base unknown malware analysis service with guaranteed protection signature delivery time not more than 5 minutes and should be supplied with on premise solution.	Mandatory	1(Max)			
220.	The solution must be able to use AV and zero day signatures based on payload and not just by hash values and it should support bare metal analysis if required. The advanced malware analysis (malware sandboxing) solution must have MacOS and Linux executable scanning by default.	Weightage	Yes- 5 Mark (Max) No - 0 Mark			
221.	The protection signatures created base unknown malware emulation should be payload or content base signatures that cloud block multiple unknown malware that use different hash but the same malicious payload.	Mandatory	1(Max)			
222.	The solution must be able to use AV and zero day signatures based on payload and not just by hash values and it should support bare metal analysis if required using hybrid setup.	Mandatory	1(Max)			
223.	Advance unknown malware analysis engine should be capable of machine learning with static analysis and dynamic analysis engine with custom-built virtual hypervisor analysis environment	Mandatory	1(Max)			

224.	Advance unknown malware analysis engine with real hardware, detecting VM-aware malware to detect and protect from virtual sandbox evading advance unknown malware. The device should support 24 VMs and at least 2X 2TB in RAID1	Mandatory	1(Max)			
225.	OEM data lake base unknown malware analysis service should be certified with SOC2 or any other Data privacy compliance certification for customer data privacy protection which is uploaded to unknown threat emulation and analysis	Mandatory	1(Max)			
226.	Able to detect and prevent zero day threats infection through HTTP, HTTPS, FTP, SMTP, IMAP use by any of application used by the users (e.g.: Gmail, Facebook, MS outlook)	Mandatory	1(Max)			
227.	Advance unknown malware analysis engine should be capable of machine learning with static analysis and dynamic analysis engine with custom-built virtual hypervisor analysis environment	Mandatory	1(Max)			
228.	Advance unknown malware analysis engine should be able to creates automated high-fidelity signature for command and control connections and spyware to inspect command and control HTTP payload to create one to many payload base signatures protection from multiple unknown spyware and command and control channels using single content base signature	Mandatory	1(Max)			
229.	The protection signatures created base unknown malware emulation should be payload or content base signatures or STIX format that cloud block multiple unknown malware that use different hash but the same malicious payload.	Mandatory	1(Max)			
230.	APT appliance should support IPv6 connections	Weightage	Yes-5 Marks(Max) No-0			
231.	The APT should assist the team in discovering the infected host by providing Detailed analysis of every detected malicious file and Session data associated with the delivery of the malicious file, including source, destination, application, User and URL etc.	Mandatory	1(Max)			
232.	The APT should integrate with same OEM Next Generation Firewall and support open API for integration SIEM tools etc.	Weightage	Yes-5 Marks(Max) No-0			
233.	Single device should be capable of integrating with at least 50 NGFW and should support clustering of up to 4 units.	Weightage	Yes-5 Marks(Max) No-0			
SSL and SSH Decryption: 9 Marks						
234.	Equipment Test Certification: FCC Class A, CE Class A, VCCI Class A, CB or Common Criteria Certified..	Mandatory	1(Max)			
235.	SSL decryption in Hardware and shall be able to identify, decrypt and evaluate SSL traffic in an outbound connection (forward-proxy)	Mandatory	1(Max)			

236.	Identify the amount of TLS traffic, non-TLS traffic, decrypted traffic, and non-decrypted TLS traffic, number of SSL sessions in a separate section for c better visibility and troubleshooting. Next Generation Firewall should also show decryption failure (if any) reason data in GUI for troubleshooting	Mandatory	1(Max)			
237.	Identify, decrypt and evaluate SSH Tunnel traffic in an inbound and outbound connections	Mandatory	1(Max)			
238.	Capability to be configured and deployed as SSL connection broker and port mirroring for SSL traffic	Mandatory	1(Max)			
239.	Supports TLSv1.3 decryption in all modes (SSL Forward Proxy, SSL Inbound Inspection, Broker and SSL Decryption Port Mirroring.	Mandatory	1(Max)			
240.	Ability to have a SSL inspection policy differentiate between personal SSL connections i.e. Banking, shopping, health and non-personal traffic	Mandatory	1(Max)			
241.	Identify, decrypt and evaluate SSL traffic in an inbound connection	Mandatory	1(Max)			
242.	SSL decryption must be supported on any port used for SSL i.e. SSL decryption must be supported on non-standard SSL port as well	Mandatory	1(Max)			
NAT: 1 Mark						
243.	Support • Network Address Translation (NAT) • Port Address Translation (PAT) • Dual Stack IPv4 / IPv6 (NAT64)	Mandatory	1(Max)			
IPv6: 1 Mark						
244.	Support IPv6-: • Port oversubscription • Firewall policy with User and Applications • SSL Decryption • Administration of Gateway and Management solutions • DHCP • ECMP	Mandatory	1(Max)			
Routing and Multicast Support: 20 Marks						
245.	Support VXLAN Tunnel content inspection	Mandatory	1(Max)			
246.	The proposed solution must support Policy Based forwarding/ Policy based Routing based on: - Zone - Source or Destination Address - Source or destination port - Application (not port based) - AD/LDAP user or User Group - Services or ports	Mandatory	1(Max)			

247.	Support the ability to create QoS policy on a per rule basis: -by source address -by destination address -by application (such as Skype, Bittorrent, YouTube, Azureus) -by static or dynamic application groups (such as Instant Messaging or P2P groups) -by port and services	Mandatory	1(Max)			
248.	Support VPN Tunnel Interfaces as well as GRE tunnels.	Weightage	Yes-5 Marks(Max) No-0			
249.	Support DHCP Client configuration & DHCP Server configuration.	Mandatory	1(Max)			
250.	Bidirectional Forwarding Detection (BFD)	Mandatory	1(Max)			
251.	VOIP Applications Security by supporting to filter SIP, H.323, MGCP and Skinny flows.	Weightage	Yes-10 Marks(Max) No-0			
Authentication: 3 Marks						
252.	NGFW should support the following authentication protocols: LDAP, Radius, and Kerberos. Solution must have inbuilt integration (AD/ LDAP) for Identity based policies without any external devices. AD/LDAP integration shall work without any additional VM dependency.	Mandatory	1(Max)			
253.	Firewall's SSL VPN shall support the LDAP, Radius, Kerberos, SAML authentication protocols	Mandatory	1(Max)			
254.	Acquire User Identities from: LDAP, Captive Portal, VPN, NACs (XML or API), Syslog, Terminal Services, XFF Headers, Server Monitoring, AND client probing	Mandatory	1(Max)			
Monitoring, Management and Reporting: 30 Marks						
255.	Allow single policy rule creation for application control, user based control, host profile, threat prevention, Anti-virus, file filtering, content filtering, QoS and scheduling at single place within a single rule and not at multiple locations. There must not be different places and options to define policy rules based on these parameters.	Weightage	Yes-5 Marks(Max) No-0			
256.	Offer dynamic capabilities that monitors proposed security gateways, policies and configuration settings all in real time which in turns helps Bank to easily map against security best practices and guide admins to adhere to same for strengthening the security posture of the Bank.	Mandatory	1(Max)			
257.	The NGFW Central Management platform must support up to 20k logs per second. Solution must support management of multiple security layers, providing superior policy efficiency and enabling you to manage security through a single pane of glass.	Weightage	Yes-5 Marks(Max) No-0			

258.	The management solution must have the native capability to optimize the security rule base and offer steps to create application based rules. Solution should correlates logs from all gateways to identify suspicious activity, track trends and investigate/mitigate events – all through a single plane of glass		Mandatory	1(Max)			
259.	1 virtual/hardware centralized management solution in DC and DR each with 2 TB of storage		Mandatory	1(Max)			
260.	Should have separate real time logging base on all Traffic, Threats, User IDs, Data filtering, Content filtering, unknown malware analysis, Authentication, Tunneled Traffic and correlated log view base on other logging activities .The NGFW Central Management platform must support up to 20k logs per second		Weightage	Yes-10 Marks(Max) No-0			
261.	Report generation on a manual or schedule (Daily, Weekly, Monthly, etc.) basis		Mandatory	1(Max)			
262.	Should allow the report to be exported into other format such as PDF, HTML, CSV, XML etc.		Weightage	Yes-5 Marks(Max) No-0			
263.	Should have built in report templates base on Applications, Users, Threats, Traffic.		Mandatory	1(Max)			
Total Marks				**231 Marks(Max)**			
Application Delivery Controller (ADC) with Threat Intelligence Gateway and SSL/TLS Offloader							
Minimum Core Specifications: 10 Marks							
264.	CPU	24 Physical Cores	Mandatory	1(Max)			
265.	RAM	256 GB	Mandatory	1(Max)			
266.	Storage	SSD Storage with minimum 500GB. Bidder/OEM may increase the size depending upon box capacity	Mandatory	1(Max)			
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	Mandatory	1(Max)			
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	Mandatory	1(Max)			
269.	Power on demand	Hot Swappable redundant power supply	Mandatory	1(Max)			

270.	SSL Offloading	60 Gbps Scalable upto 90 Gbps (without any additional hardware)	Mandatory	1(Max)			
271.	Ports	4*100G 16*25G	Mandatory	1(Max)			
272.	Form Factor	1RU (Preferably)	Mandatory	1(Max)			
273.	Instances (Isolated)	20 scalable upto 35 (without any additional hardware)	Mandatory	1(Max)			
Other Features: 36 Marks							
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.		Mandatory	1(Max)			
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		Mandatory	1(Max)			
276.	Always on management & LED to initial configuration.		Mandatory	1(Max)			
277.	Instance should have different OS version, configuration and should be able to allocate CPU, Memory, Hard disk. Rebooting one instance should not affect other instance.		Mandatory	1(Max)			
278.	The performance of SSL TPS must be mentioned in public data sheet. SSL TPS number should be without SSL key reuse.		Weightage	Yes-5 Marks(Max) No-0			
279.	Application-level load balancing including the ability to act as HTTP 2.0 based Application Load balancer so that it can integrate with next-gen API Based Applications, Mobile Applications and micro-service/container-based applications.		Mandatory	1(Max)			
280.	TLSv1.2 and TLSv1.3 on both Client and Server side to secure separate Transport Layer security during remote-end and application communication.		Mandatory	1(Max)			
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.		Mandatory	1(Max)			
282.	The architecture must be with HTTP Keep-Alive to allow the load balancer system to minimize the number of server-side TCP connections by making existing connections available for reuse by other clients for TCP optimization to reduce the traffic towards backend application servers which enhance server & application performance. Bidder must mention the function.		Weightage	Yes-5 Marks(Max) No-0			

283.	TCP communication optimization so that for slow remote end users should have better application access experience without impacting back-end application server connection holding time extension/resource utilization. Bidder must mention the function.	Weightage	Yes-5 Marks(Max) No-0			
284.	Server load balancing algorithms like (but not limited to) round robin, weighted round robin, least connection, Persistent IP, Hash IP, hash Cookie, consistent hash IP, shortest response, proximity, SNMP, SIP session ID, hash header, Observed, Predictive, least session, least connections, super HTTP, least latency, weighted round robin and TCL based script for customized algorithm etc.	Mandatory	1(Max)			
285.	The Load Balancer shall distribute traffic efficiently while ensuring high application availability. It shall monitor server health to determine that application servers are not only reachable but alive. If the Load Balancer detects issues, it shall automatically remove downed servers from the server pool and rebalance traffic among the remaining servers.	Mandatory	1(Max)			
286.	Load balancing capacity to add unlimited new back-end server as member of load-balancing group and prioritize the traffic to send new back-end servers. Also, it should have mechanism to remove the back-end server from pool by gracefully without hampering any remote user connection so that existing user communication must not be disconnected during maintenance or troubleshooting window which will help more application availability.	Mandatory	1(Max)			
287.	The Load Balancer shall improve the user's experience by increasing server response time. Shall support Caching web content that saves network bandwidth requirements and reduce loads on backend web servers.	Mandatory	1(Max)			
288.	Support ICAP integration with other security devices to improve security.	Weightage	Yes-5 Marks(Max) No-0			
289.	Script-based functions support for content inspection, traffic matching and monitoring of HTTP, XML, generic TCP. Load balancer should support Policies to customize new features in addition to existing feature/functions of load balancer	Mandatory	1(Max)			
290.	The Load Balancer Shall have full traffic control and be able to route requests to servers based on region, device, browser, or several other factors. This enables organization to deliver customized application responses to users.	Mandatory	1(Max)			
291.	To maximize outbound bandwidth, the Load Balancer shall automatically compress content to minimize network traffic between application servers and the end user browser to offload the compression workload from back-end application server to enhance application server performance.	Mandatory	1(Max)			
292.	Perform TCP multiplexing and TCP optimization, SSL Offloading with SSL session & persistency mirroring, HTTP Compression, caching etc. in active-passive high-availability mode.	Mandatory	1(Max)			

293.	High Availability for both TCP session mirroring and SSL session mirroring in full-proxy (Forward Proxy and Reverse Proxy) mode in Active-Standby HA Architecture.		Mandatory	1(Max)			
Other requirements from OEM & Bidder: 7 Marks							
294.	The OEM/Manufacturer should have ISO 9001, ISO 14001, and ISO 27001 Certification. Bidder must submit the OEM's certificates.		Mandatory	1(Max)			
295.	Respective bidder also needs to ensure that the final deployment of the Web & API application security solution is done based on the standards design guideline and best practices keeping in mind the DC compliance requirements and operational requirements.		Mandatory	1(Max)			
296.	Bidder has to ensure that the final deployment is done by the OEM certified resources to validate design standards and best practices.		Mandatory	1(Max)			
297.	Bidder must submit the required performance document and compliance reference document for the proposed solution.		Mandatory	1(Max)			
298.	Bidder must provide the detail compliance report with reference. The reference URL / information of RFP technical specification compliance should be publicly available, referenceable, and accessible document.		Mandatory	1(Max)			
299.	Manufacturer's warranty part number should be mentioned, minimum 3 (three) Full years' warranty for technical solution support with Patch & New Software Upgrade, RMA replacement should be provided for the proposed solution from the date of commissioning.		Mandatory	1(Max)			
300.	Support active-active and active-backup high availability		Mandatory	1(Max)			
SSL Inspection							
301.	CPU	Minimum 24 Physical Cores	Mandatory	1(Max)			
302.	Storage	Minimum 2x 1TB U.2 Enterprise-class SSD (RAID 1 Mirrored)	Mandatory	Storage Capacity 200% or more than proposed minimum – 3 Marks(Max) Else 1 Mark			
303.	RAM	Minimum 256 GB	Mandatory	1(Max)			
304.	Power on demand	Dual AC/DC supply with hot swappable units, with always on management & LED to initial configuration	Mandatory	1(Max)			
305.	Form Factor	1RU/2RU in standard 42U Rack	Mandatory	1(Max)			
306.	Ports	4*100G ports and 16*25G/10G with negotiable to 10G with SFP+/ QSFP+ as per the compatible interfaces	Mandatory	1(Max)			

307.	Device should feed decrypted traffic to security device in service chain for inspection received from end user and encrypt before sending it to back end application.		Mandatory	1(Max)			
308.	Should support encryption and decryption for TLS 1.3,1.2 and SSL traffic with ECC, RSA cipher support.		Mandatory	1(Max)			
309.	Should support 200K SSL TPS of 2048 key size. Device should support both L2 and L3 deployment with ICAP support		Mandatory	1(Max)			
310.	Device should provide ADC functionality as mentioned in RFP and should support virtualization.		Mandatory	1(Max)			
311.	L7 throughput of device should be minimum 180 Gbps		Mandatory	1(Max)			
312.	Solution should provide all functionality on single OS instance and hardware and software should be from same OEM		Mandatory	1(Max)			
313.	Solution should able to categorize internet outbound traffic including office 365.		Mandatory	1(Max)			
		TOTAL		**15 Marks(Max)**			
Total Marks				**68 Marks (Max)**			
Web Application Firewall (WAF)							
Minimum Core Specifications: 12 Marks							
314.	CPU	24 Physical Cores	Mandatory	1(Max)			
315.	RAM	256 GB	Mandatory	1(Max)			
316.	Storage	Minimum SSD Storage: 500GB	Mandatory	1(Max)			
317.	Throughput	20Gbps	Mandatory	1(Max)			
318.	Throughput Scalability (without any additional hardware)	50Gbps	Mandatory	1(Max)			
319.	Latency	<8 µs	Mandatory	1(Max)			
320.	Power on demand	Hot Swappable redundant power supply	Mandatory	1(Max)			
321.	Form Factor	1RU (Preferably)	Mandatory	1(Max)			
322.	Ports	4*100G ports and 16*25G/10G with negotiable to 10G with SFP+/ QSFP+ as per the compatible interfaces	Mandatory	1(Max)			
323.	Licenses	Unlimited. Unrestricted	Mandatory	1(Max)			
324.	Protocols	SNMPv3, Syslog	Mandatory	1(Max)			
325.	Domains	64	Mandatory	1(Max)			
Features: 128 Marks							
326.	Proactive BOT defence		Mandatory	1(Max)			
327.	BOT signatures based detection		Mandatory	1(Max)			
328.	The Bot mitigation not be limited to reputation-based/ signature based controls		Mandatory	1(Max)			

329.	Support different policies for different applications based on host name or per application path	Mandatory	1(Max)			
330.	Offer parameters and hidden form fields (Static/Dynamic) obfuscation and protection against manipulation.	Mandatory	1(Max)			
331.	Credential protection of all types.	Weightage	Yes-5 Marks(Max) No-0			
332.	Support all major cipher suites like Camellia Ciphers Suites, SSLv3 and TLSv1.3	Mandatory	1(Max)			
333.	Ability to merge automatically built security policy with a manually built security policy or policy built from Industry Standard Dynamic Analysis Security Testing (DAST) tools XML report and must support integration with industry leading Dynamic Analysis Security Testing (DAST) tools of IBM, Microfocus, Rapid7 etc. to perform virtual patching for its protected web applications.	Mandatory	1(Max)			
334.	Support both the positive and negative security model approach.	Weightage	Yes-5 Marks(Max) No-0			
335.	Address and mitigate the OWASP Top Ten web application security vulnerability.	Mandatory	1(Max)			
336.	Specially to protect against the of the most seen application vulnerabilities. This currently includes: 1. Injection attacks 2. Broken Authentication 3. Sensitive data exposure 4. XML External Entities (XXE) 5. Broken Access control 6. Security misconfigurations 7. Cross Site Scripting (XSS) 8. Insecure Deserialization 9. Smarter bot detection using machine learning 10. Robust and rapid attack response 11. Advanced dashboard capabilities 12. Real-time actionable threat intelligence 13. Missing Function Level Access Control 14. Cross-Site Request Forgery (CSRF) 15. Password spraying 16. Invalidated Redirects and Forwards	Mandatory	1(Max)			

337.	Support custom security rules. Administrators should be able to define rules for the positive and negative security model and to create correlation rules with multiple criteria. If this requires any script/config changes to be enabled, same needs to be provided as part of overall solution without having any external dependencies.	Mandatory	1(Max)			
338.	Capable of Webshell/ Backdoor Detection.	Weightage	Yes-5 Marks(Max) No-0			
339.	Inspection and protection for WebSocket and Secure WebSocket of application.	Mandatory	1(Max)			
340.	WAF should have capability of Proactive BOT Defence (both detection and Protection) mechanism beyond signatures and reputation to accurately detect malicious and benign bots using client behavioural analysis, server performance monitoring, and escalating JavaScript and CAPTCHA challenges or equivalent. The BOT defence feature should have Predefined Bot Defence profile to enable quicker and easier BOT defence configuration. The signature should be updated regularly, and bidder must ensure signature and threat database update subscription license for entire contract duration.	Mandatory	1(Max)			
341.	Brute Force attack detection by CAPTCHA challenges to clients and should be capable to redirecting Brute force attack traffic to Honey Pot page/System.	Mandatory	1(Max)			
342.	Detect attacks trying to bypass the CAPTCHAS by farming out the CAPTCHA images to pools of user that respond.	Mandatory	1(Max)			
343.	In-built security engine to address complex attacks that are ambiguous in nature. It must also examine multiple pieces of information at the network, protocol & application levels over time & correlate them to distinguish between attacks & valid user traffic.	Mandatory	1(Max)			
344.	Capable to obfuscate sensitive field names to defeat Man-in-The-Browser Attacks.	Mandatory	1(Max)			
345.	Protection against Layer 7 Application DDOS type of attacks in full-Proxy Mode (Forward Proxy and Reverse Proxy) using machine learning mechanism form day 1.	Mandatory	1(Max)			
346.	Behavioural DoS mitigation Technology to detect DDOS attacks without human intervention.	Mandatory	1(Max)			
347.	Protection against viral/infected file uploads through ICAP integration with 3rd party/antivirus/Sandbox solution.	Mandatory	1(Max)			
348.	Include a pre-configured list of comprehensive and accurate web attack signatures.	Mandatory	1(Max)			

349.	Signature staging feature for new signature update which will apply the new signatures to the web application traffic but does not block the application by trigger those new attack signatures. This feature is required to reduce the number of violations triggered by false-positive matches regarding new signature update.	Mandatory	1(Max)			
350.	CSRF checkbox attack protection and mitigate Buffer overflows.	Mandatory	1(Max)			
351.	Rate Limiting for Client and Application communication to limit the TCP communication during DDoS Attack.	Mandatory	1(Max)			
352.	Protection against • Cross-site Request Forgery. • Web worm protection • Website cloaking • Outbound data theft	Mandatory	1(Max)			
353.	Detect and block request coming from anonymous proxies.	Weightage	Yes-10 Marks(Max) No-0			
354.	Daily automatic update of signature service and apply the new signatures. Before enforcing the new signature, there should be a feature to test as staging mode for application protection.	Mandatory	1(Max)			
355.	Capability of Geo Location Blocking and should be able to take threat intelligence feed to reveal inbound communication with malicious IP addresses and enable granular threat reporting and automated blocking. The IP address database should be update periodically.	Weightage	Yes-10 Marks(Max) No-0			
356.	"Cloak" error responses to hide sensitive server related information in the response body and response headers.	Mandatory	1(Max)			
357.	The solution profiling technology should be able to detect and protect against threats which are specific to the custom code of the web application. After the learning phase, the solution must be able to understand the structure of each protected URL and must be able to detect deviations and various anomalies (or violations) and block attacks on the custom code of the application.	Mandatory	1(Max)			
358.	Profiling of JSON. HTTP requests in the JSON format must be learnt by the WAF with the parameters and values.	Mandatory	1(Max)			
359.	Protect web applications that include Web services (XML) content.	Mandatory	1(Max)			
360.	a) Automatically update Certificate bundles from the appropriate CAs without any user intervention OR b) Appliance should maintain certificate and key repository	Mandatory	Supports a -5 Marks(Max) Supports b- 2 Mark			
361.	The solution should provide a mode whereby it can rewrite HTTP applications to HTTPS on-the-fly, e.g., by modifying all outbound content, and redirect incoming HTTP requests to the HTTPS.	Mandatory	1(Max)			

362.	The solution should protect session tokens, i.e., cookies: a. Sign cookies, to prevent clients from changing them b. Encrypt cookies, to hide contents. c. Prevent Cookie Replay attacks d. Allow for exempting certain cookies from security checks	Mandatory	1(Max)			
363.	The solution should support protection of XML Web Services with common web application as well as XML specific attacks.	Mandatory	1(Max)			
364.	It should be possible to force conformance with full WS-I Basic specification.	Mandatory	1(Max)			
365.	The solution should provide for validating XML Documents and protecting against XML, DOS and injection attacks (SQL, OS, XSS injection, etc.).	Mandatory	1(Max)			
366.	The solution should provide for validating SOAP messages, headers, and body against a WSDL schema.	Mandatory	1(Max)			
367.	Data analytics on application usage, including malicious or suspect activity.	Mandatory	1(Max)			
368.	The solution must support regular expressions for the following purposes: - Signature definition - Sensitive data definition - Parameter type definition - Host names and URL prefixes definition - Fine tuning of parameters that are dynamically learnt from the web application profile.	Mandatory	1(Max)			
369.	The solution must be able to decrypt SSL web traffic that are using Diffie-Hellman key exchange protocols with the monitoring appliance deployed in transparent layer-2 mode. The solution must be able to support Proxy SSL functionality also wherein the WAF will be able to inspect the SSL traffic without offloading it on to itself.	Mandatory	1(Max)			
370.	The solution must have API inspection, rate limiting, behavioural analysis, anti-automation, detects application program interface (API) threats and API protocol security check to secure REST API, JSON, XML/SOAP and Gateway APIs.	Mandatory	1(Max)			
371.	The solution must support masking of sensitive data in alerts.	Weightage	Yes-5 Marks(Max) No-0			
372.	The solution should integrate with syslog to work with any solution and support known log formats.	Mandatory	1(Max)			
373.	The solution should support integration with any onsite hosted or cloud based SIEM tools. Integration with SIEM should be done by OEM/Local Partner	Mandatory	1(Max)			
374.	The proposed WAF should provide PCI DSS compliance reporting.	Mandatory	1(Max)			
375.	The solution should provide HTTPS interface management for administering the device.	Mandatory	1(Max)			
376.	The solution should provide SSH interface management for administering the device.	Mandatory	1(Max)			

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.	Weightage	Yes- 5 Mark(Max) No- 0 Mark			
378.	The solution must allow administrators to add & modify signatures.	Mandatory	1(Max)			
379.	The entire management solution must have a dedicated central management system to centrally all devices.	Mandatory	1(Max)			
380.	The Management solution must have HTTP and TCP traffic analytic reports to identify application performance issues and network troubleshooting issues along with traffic report.	Mandatory	1(Max)			
381.	The entire management solution must be capable to store all the logs (request, response parameters). The log database system must be separated and redundant so that if the central management module is down, the logs should not be missed.	Mandatory	1(Max)			
382.	The solution must allow the user to use a standard browser to access the management UI. Management system can be a physical or virtual appliance. In case of virtual appliance offering bidder must mention required hardware details.	Mandatory	1(Max)			
383.	The solution support role-based admin access with roles like no access, Guest, Operator, Application editor, Resource Administrator, Administrator or equivalent to achieve the objective	Mandatory	1(Max)			
384.	Able to auto sync setup and synchronization of multiple devices thus eliminating difficult hierarchical management common to DNS	Mandatory	1(Max)			
385.	Provides global high availability and reliability of applications across multiple sites and ensures application availability by tracking and managing inter-dependencies between applications.	Mandatory	1(Max)			
386.	Should be supplied with inbox or centralized management-CLI, GUI for policy configuration and verification	Mandatory	1(Max)			
387.	Supports DNS A, AAAA record	Mandatory	1(Max)			
388.	Supports static route table and optional dynamic routing such RIP, OSPF, IS-IS, BGP	Mandatory	1(Max)			
389.	Supports multiple firmware and firmware uploads without resetting device	Weightage	Yes-10 Marks(Max) No-0			
390.	Able to cache DNS responses	Mandatory	1(Max)			
391.	Able to provide flexibility in having deterministic probers which communicate with each node to determine (depending on the probe or monitor configured) its availability, status, proximity, or responsiveness.	Mandatory	1(Max)			
392.	Able to perform intelligent probing of your network resources to determine whether the resources are up or down. This allows you to specify which device probe specific servers for health and performance data.	Mandatory	1(Max)			

393.	Able to inform administrator of query stats of device groups in synchronization to improve visibility, management and troubleshooting of groups	Mandatory	1(Max)			
394.	Able to support composite monitors, such as M of N rule (e.g., need only 2 successes out of 3 monitors).	Mandatory	1(Max)			
395.	Able to support static and dynamic load-balancing algorithms such as: • Round robin • Global availability • LDNS persistence • Application availability • Geography • Virtual server capacity • Least connections • Packets per second • Round trip time • Hops • Packet completion rate • User-defined QoS • Dynamic ratio • LDNS • Ratio • Kilobytes per second • RADIUS accounting	Mandatory	1(Max)			
396.	Supports built-in GEO-Location database for accurate Geo load balancing. The default database shall provide geolocation data for IPv4 addresses at the continent, country, state, based on IP Address available. This also allows user to define how traffic is routed based on this information.	Mandatory	1(Max)			
397.	Support intelligent routing with load balancing geography-based distribution via programmatic control	Mandatory	1(Max)			
398.	Able to support mixed combinations of IPv6 and IPv4 virtual addresses and nodes resolving AAAA queries without requiring wholesale network and application upgrades. This provides DNS gateway and translation services for hybrid IPv6 and IPv4 solutions and manages IPv6 and IPv4 DNS servers in DNS64 environments.	Mandatory	1(Max)			
399.	Able to support application-centric monitoring, persist user connections across applications and data centers and be automatically routed to the appropriate data center or server, based on application state, ensuring that users are directed back to the same site regardless of their entry point.	Mandatory	1(Max)			

400.	Able to propagate the desired persistence information to local DNS servers, reducing the required frequency of synchronizing back-end databases and maintain session integrity.		Mandatory	1(Max)			
401.	Supports DNS fallback in case GLSB decision is not available		Mandatory	1(Max)			
402.	Deliver high speed standard (non-GSLB) DNS query responses. Proposed DNS solution must be capable of 1000000 DNS response per second from day 1.		Mandatory	1(Max)			
Other requirements from OEM & Bidder: 2 Marks							
403.	The OEM/Manufacturer should have ISO 9001, ISO 14001, and ISO 27001 Certification. Bidder must submit the OEM's certificates.		Mandatory	1(Max)			
404.	All components of the solution should be capable of both Active-Active and Active Passive High Availability and the feature should be enabled from Day 1		Mandatory	1(Max)			
Total Marks				**142 Marks (Max)**			
Perimeter analytics – NDR (Network Threat Detection & Response)							
Minimum Core Specifications: 8 Marks							
405.	Storage	Dual Hot swappable Storage Memory Capacity of atleast 2 x 4TB SSD or 7.2k RPM HDD. Bidder has to factor storage as per the scope defined in the RFP by the Bank	Mandatory	SSD-5 Marks HDD-2 marks			
406.	Throughput	Threat prevention - 20 Gbps (rated multi-protocol throughput including HTTP, SMTP,SMB, FTP, RDP and other protocols)	Mandatory	1(Max)			
407.	Throughput Scalability (without/ with any additional hardware)	Throughput Scalability (without/with any additional hardware) Inline Web Traffic Analysis - atleast 40 Gbps (rated HTTP throughput)(rated multi-protocol throughput including HTTP, SMTP,SMB, FTP, RDP and other protocols)	Mandatory	1(Max)			
408.	Ports	Minimum 8x10/25/40 GE copper or fiber ports	Mandatory	1(Max)			
Key Requirements: 16 Marks							
409.	Able to detect multiple infection vectors (Network, Files, https, http) as a dedicated purpose-built platform deployed independently without any functional reliance on existing layers of security like NGFW, NGIPS, Proxy etc. adhering to defence in depth architecture, where, If any of the layers of core underlying security get replaced or non-functional, the proposed solution must be capable to function on its own.		Mandatory	1(Max)			

410.	The entire solution should preferably be from a single OEM or multiple OEMs ensuring that the integrated platform requirements are achieved.	Weightage	Single OEM-10 Marks(Max) 2 OEMs-5 Marks More than 2 OEMs- 1 Mark			
411.	Detect zero-day, multi-stage, fileless and other evasive advanced attacks using dynamic, signature-less analysis in a safe, anti-evasive execution environment. The solution should be sized appropriately by the bidder including all other costs required for performance, scalability and efficiency.	Mandatory	1(Max)			
412.	On-premise, easy-to-manage, clientless platform that deploys quickly and involves minimal or no dependency on customization and management. It must not be requiring any complex rules, policies or customization, tuning to filter & forward the traffic for delivering the core solution functionality. The solution must preferably be proposed as physical appliance while central management can be deployed on Virtual hypervisor(VMware Esxi or MS Hyper-V or KVM) ensuring performance and applicability to environment.	Mandatory	1(Max)			
413.	Automated payload analysis covering entire network landscape, bidders must propose the payload analysis solution on-premise covering threat analysis for major Operating Systems (windows, Macintosh and Linux) with required Applications as part of the Execution environment. The analysis environment must be purpose built, deployed, and maintained for patch updates and firmware upgrades by the OEM.	Mandatory	1(Max)			
414.	Integrated regular security threat intelligence content subscription as part of the solution for the period of contract or it's extension. The security content must be integrated in a non-sharing (one-way) mode, without requirement to send any file or data to OEM cloud for analysis or verdicts.	Mandatory	1(Max)			
415.	NDR should have well defined work flow for response mechanism	Mandatory	1(Max)			
Network Traffic & Payload Analysis (Realtime/ Near Realtime): 55 Marks						
416.	Integrate with an enterprise grade SSL orchestration solution for traffic decryption to archive the SSL inspection for north-south traffic.	Mandatory	1(Max)			
417.	Support an inline monitoring mode, blocking mode preferably along with Inline Proxy, TAP/SPAN, ICAP etc. or by using third party integration such as SOAR/API or any other means	Mandatory	Inline blocking – 7 Marks(Max), Direct Integration with other device - 4 Marks API integration -1 Mark			

418.	Inline monitoring or blocking mode that automatically blocks inbound exploits and malware by using third party integration such as SOAR/API or any other means or by using inbuilt capabilities	Mandatory	Inline blocking – 7 Marks(Max), Direct Integration with other device - 4 Marks API integration -1 Mark			
419.	Component is a secured purpose built hypervisor as during execution analysis of files, objects, flows, attachments, URL's the environment unleashes any hidden or targeted advance malware attacks. The attacks should not be able to evade the environment leading to poor detection & false negative scenarios.	Mandatory	1(Max)			
420.	Each component has its own dedicated Analysis capability with all dependencies viz; additional licenses, customization or infrastructure to run exclusively on-premise.	Weightage	Yes-5 Marks(Max) No-0			
421.	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.	Mandatory	1(Max)			
422.	The Internal Network Analysis solution should also be able to detect malicious post-exploitation activities such as attacker lateral movements between various zone like user workstation & servers. The solution should detect lateral movement indicating source & destination IP addresses, files transferred, commands executed, with detailed execution analysis of payload, files etc.	Mandatory	1(Max)			
423.	Able to detect zero-day, multi-flow and other evasive attacks with dynamic, signature-less analysis in a safe, virtual environment and stop infection and compromise phases of the cyber-attack kill chain by identifying never-before-seen exploits and malware.	Mandatory	1(Max)			
424.	Multiple, dynamic machine learning, AI and correlation engines detect and block obfuscated, targeted and other customized attacks with contextual, rule-based analysis from real-time insights	Mandatory	1(Max)			
425.	Capability to identify malicious exploits, malware, phishing attacks and command and control (CnC) callback while extracting and submitting suspicious network traffic to the dynamic analysis engine for a definitive verdict analysis.	Mandatory	1(Max)			

426.	Dedicated engines to support server side detections, lateral movement detection and detection on post-exploitation traffic on same appliance via SPAN port traffic integration	Mandatory	1(Max)			
427.	Capable of protection against advanced attacks and malware types that are difficult to detect via signatures like web shell uploads, existing web shells, ransomware, cryptominers etc. the preventive mechanism may be achieved through inbuilt or through integration with DDoS Solution, Firewalls, NIPS or other preventive devices proposed by bidder	Mandatory	Inline blocking – 7 Marks(Max), Direct Integration with other device - 4 Marks API integration -1 Mark			
428.	Utilize multiple machine learning, AI and correlation engines represent a collection of contextual, dynamic rules engines that detects and blocks malicious activity by using third party soar/api/ or thorough internal mechanism and retroactively, based on the latest machine-, attacker- and victim- intelligence.	Mandatory	Inline blocking – 7 Marks(Max), Direct Integration with other device - 4 Marks API integration -1 Mark			
429.	The Network APT solution must detect execution of suspicious network traffic against thousands of operating system, service pack, IoT application type and application version combinations.	Mandatory	1(Max)			
430.	Capable of protection against advanced attacks and malware types that are difficult to detect via signatures like web shell uploads, existing web shells, ransomware, cryptominers etc.	Weightage	Yes-5 Marks(Max) No-0			
431.	In-built functionality to detect genuine attacks, Advanced technology engines must be used to validate alerts detected by conventional signature-matching methods to identify and prioritize critical threats.	Mandatory	1(Max)			
432.	Provide visibility to various types of network anomalies and suspicious activity such as Data Exfiltration, Beaconing, etc. and their victim attacker graphical representation at one place	Mandatory	1(Max)			
433.	Detect malicious TLS connections using a combination of available technologies	Mandatory	1(Max)			
434.	Detect Event Type for Network Anomaly, OS Change, Checksum Match, VM Signature Match, CNC Signature Match etc. logged while analyzing any traffic or pcap or objects	Weightage	Yes-5 Marks(Max) No-0			
Network Forensics (Post Compromise Investigation & Response): 70 Marks						

435.	Proposed solution should be a redundant dedicated purpose built solution that must provide full Detection, Network Visibility, Investigation & Forensic capability, through high speed lossless packet capture & analysis functions for a network traffic capture for 20 Gbps. Separate setup to be deployed for DC and DR.	Mandatory	Network Traffic capture capacity >=20 Gbps- 5 Marks(Max) else 1 Mark(Max)			
436.	Capable to provide complete packet-by-packet details pertaining to one or more session of interest including Session replay, Flow analysis, Packet decoding, Web & FTP session reconstruction, email reconstruction, image views, artefact & raw packet extractions.	Mandatory	1(Max)			
437.	Capable to classify, extract and reconstruct network activity and perform dynamic execution within a secure hardened hypervisor environment. No data should be sent to any 3rd party or open source components and cloud for any type of analysis.	Mandatory	1(Max)			
438.	The Investigation features should be provided the capability to perform complete network forensic investigations including decoding and chaining the encoded communication traffic. Also, the solution should be providing download option of select and/or bulk pcaps in industry standard formats like "pcap".	Mandatory	1(Max)			
439.	Support analytics and forensics over IPv4 and IPv6 with a capability to filter the captured packets based on layer-2 to layer-7 header information	Mandatory	1(Max)			
440.	Support password extraction from popular protocols and be able to represent user-id/password combination in addition to any related sessions executed from the node in a time-window moving forward or going back from the point of password capture or any event of interest.	Weightage	Yes-5 Marks(Max) No-0			
441.	Support Micro-tasking such as dynamic analysis by using different versions of operating systems and different versions of applications (Adobe PDF, MS be sent outside the organization for any analysis.	Mandatory	1(Max)			
442.	Provide encryption capability to ensure security of captured data packets	Weightage	Yes-5 Marks(Max) No-0			
443.	Provide network traffic insight by integrating with Rules, Indicators like IOC's or 3rd party intelligence feeds.	Mandatory	1(Max)			
444.	Classifying protocols and applications	Mandatory	1(Max)			
445.	Reconstructed file such as a Word document, Email with attachments, Image, Web page, system files	Mandatory	1(Max)			
446.	Deep-packet inspection	Mandatory	1(Max)			
447.	Traffic analysis & Aggregation	Mandatory	1(Max)			
448.	Reconstruct sessions and analyse artifacts	Mandatory	1(Max)			

449.	Scheduling Retrospective hunting & detection on historical data	Mandatory	1(Max)			
450.	Provide Reports with Single-attribute views with extensive sorting and filtering capabilities	Mandatory	1(Max)			
451.	Support capability to upload/download packet captures (PCAP's) outside the solution for analysis	Mandatory	1(Max)			
452.	Provide extensive visibility through session decoder support to view and search web, email, FTP, DNS, chat, SSL connection details and file attachments	Mandatory	1(Max)			
453.	Provide Automated processes to identify data theft, using highly trained and proven breach response analysis algorithms to diagnose potentially anomalous network behavior	Mandatory	1(Max)			
454.	Provide classification, search and real-time file extraction for instant delivery of recognizable evidence of a security breach or malware attack	Mandatory	1(Max)			
455.	Provide descriptive information about a network session including application, personal identity, intended actions, content types, file names and more	Mandatory	1(Max)			
456.	Analyse and decode leading application and file types like HTML, HTTP-GET, HTTP-POST, HTTP-RESP, SMTP, FTP, EML, DOC, DOCX, XLS, XLSX, PPT, PPTX, PDF Unencrypted IMs, Config, systeaspx, PHP, ELF) etc.	Mandatory	1(Max)			
457.	Provide an intelligent policy driven flow capture to optimize storage	Mandatory	1(Max)			
458.	Able to have Real -time indexing of all captured packets using time stamp and connection attributes	Mandatory	1(Max)			
459.	Solution should be able to capture network traffic and the data collected should be stored as PCAP or any other format for traffic analysis	Weightage	Yes- 3 Marks(Max) No- 0 Mark			
460.	Secure remote web-based GUI using HTTP for system administration	Mandatory	1(Max)			
461.	Provide system health monitoring/display via a dedicated management interface	Mandatory	1(Max)			
462.	Solution must have a dedicated on premises Malware Analysis engine with purpose built platform having windows, Linux and MAC O.S environments. Bidder may size the system as per the best available option.	Mandatory	1(Max)			
463.	Consolidate all NTA alerts along with all additional network metadata in a single workbench facilitating an immediate "one click" pivot to session data from alerts	Mandatory	1(Max)			
464.	Capability to provide Back-in-time IOC threat analysis via integration of 3rd party Threat Intelligence, STIX, and Open-IOC feeds with automated Investigation and analysis search function or integration with its own Threat Intelligence.	Mandatory	1(Max)			

465.	Web based GUI and a unified security dashboard displaying the real time consolidated data in graphical/textual format and all alerts received from and detected by all the traffic and malware analysis systems deployed in centralized/decentralized architecture. The solution should have the ability to view and identify the infected systems and drill down into infection details at centralized location..	Weightage	Yes-5 Marks(Max) No-0			
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	Mandatory	1(Max)			
467.	Proposed Solution must have an option to integrate with external enterprise SAN storage for storing raw packet data with minimum of 15000/11000 Read/Write IOPS, the appropriate solution must be provided with a Fiber HBA channel to external SAN storage. Retention period will remain same.	Weightage	Yes-10 Marks(Max) No-0			
468.	Packet Capture solution must have integrated workflow with Malware forensics platform deployed to perform execution on payload artifacts on demand.	Mandatory	1(Max)			
469.	Malware Analysis should have integrated capability for analysis of up to 8,000 analysis Per Day capacity fully on-premise and supported with minimum 6 submissions per minute and 32 parallel Sandbox VM running performance including a detailed documented REST API structure	Mandatory	1(Max)			
470.	Malware Analysis provides users with two analysis modes — live and sandbox. The solution should provide VNC or recorded reports as required by the Bank	Mandatory	1(Max)			
471.	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	Mandatory	1(Max)			
472.	Solution should facilitate export the pcap or video files for further forensics	Mandatory	1(Max)			
473.	Solution should performs deep Forensic analysis throughout the full attack life cycle and provide capability to export analysis results in an XML or PDF file	Mandatory	1(Max)			
474.	Bidders must propose a solution on premise which is easy-to-manage, clientless platform that gets deployed quickly and involves minimal or no dependency on customization and management of operating environment.	Mandatory	1(Max)			
475.	Solution must not be requiring any complex rules, policies or customization, tuning to filter & forward of the traffic to 3rd party or other solution components to deliver its core functionalities.	Mandatory	1(Max)			

476.	Proposed malware forensic Analysis engine must provide in-house analysts with a full 360-degree view of an attack, from the initial exploit to callback destinations and follow on binary download attempts.	Mandatory	1(Max)			
477.	System should have API integration with proposed all types of firewall/ NIPS, illegitimate traffic can be denied any of the prevention mechanism deployed by bidder. Bidder may choose to deploy combination of prevention device such as FIREWALL/Anti DDOS/NIPS or any other control mechanism as part of automatic Realtime or near real time response mechanism	Mandatory	1(Max)			
File Analysis - FTP/SFTP shares within Data Centers: 5 Marks						
478.	Device should be dedicated file analysis solution with agentless analysis engine to detect zero-day, advance APT attacks and other evasive attacks using dynamic, signature-less analysis.	Mandatory	1(Max)			
479.	Support agentless scanning of storages using protocols like CIFS, WebDAV, sharepoint, NFS-compatible file shares, etc, without affecting performance of DAT servers.	Weightage	Yes- 2 Marks(Max) No-0 Mark			
480.	File analysis component solution should also have the capability to be deployed in scenarios where users have the provision of uploading files directly from untrusted zones to trusted zones inside Datacentre. The solution should provide a mechanism to analyze all files getting uploaded through Web or FTP portals.	Mandatory	1(Max)			
481.	On-demand scanning, continuous scanning, selective file scanning and off box scanning of external drives, servers, devices etc. for advance malware threats.	Mandatory	1(Max)			
Central Management Console and Reporting: 29 Marks						
482.	Central Management intelligence in high availability mode at DC to manage and administrate the overall deployed ecosystem, ensuring that sensors, components & appliances share the latest intelligence and correlate across attack vectors to detect and prevent cyber incidents.	Mandatory	1(Max)			
483.	Central management solution must help centralize the entire deployment management into a single console to manage configurations, threat updates, and software upgrades	Mandatory	1(Max)			
484.	Central management solution must have capability to enable remote management and dynamic configurations	Mandatory	1(Max)			
485.	Central management solution must enables blended threat prevention using multi-vector correlation of collected data events	Mandatory	1(Max)			
486.	Central management solution must be able to distribute and disseminate in real-time local threat intelligence to multiple deployments across your systems in an automated fashion	Mandatory	1(Max)			

487.	Central Management must be supplied with minimum 2x 1GigE BaseT Network interfaces ports with a separate dedicated Management & IPMI ports, having minimum storage capacity of 4 x 4 TB HDD, on RAID 10/RAID5/RAID6 with minimum usable storage of 8TB and redundant power supply.	Mandatory	1(Max)			
488.	Solution must only be accessible via web UI and shall not require any plugins or thick client requirements for Admins or Analysts to access and manage.	Mandatory	1(Max)			
489.	Support SNMP, syslog etc. for integration with all leading SIEM/SOC solutions. The Solution components should also be providing access over REST API's with detailed OEM documentation. The Solution must only be accessible via web UI and shall not require any plugins or thick client requirements for Admins and Analysts access.	Mandatory	1(Max)			
490.	Monitoring/prevention of Internet based traffic, Reporting and analytics should be in place for real-time monitoring of the egress and ingress traffic to understand 360 degree view. Prevention by using third party integration such as SOAR/API or any other means or by using inbuilt capabilities.	Mandatory	Automatic Inline blocking – 10 Marks(Max), Direct Integration with other device - 3 Marks API integration -2 Mark			
491.	Network traffic inspection to detect exploitation of vulnerabilities (both known and Zero-days)	Mandatory	1(Max)			
492.	Network traffic inspection to detect suspicious activities which are not limited to as DGA, Use of Remote access software tools, Adware, Trojans etc.	Mandatory	1(Max)			
493.	Network traffic inspection to detect suspicious activities such as different malware family used by Threat Actor groups, TTPs used for malicious activities and lateral movements	Mandatory	1(Max)			
494.	All components of the solution should be capable of both Active-Active and Active-Passive High Availability and the feature should be enabled from Day 1	Mandatory	1(Max)			
495.	Solution must provide a robust GUI based analysis interface having alerts populated with relevant metadata, MD5, SHA256, Malicious object, summary, Mitre techniques, Sandbox Analysis details, threat analysis graph, Pcap, and other relevant email metadata.	Mandatory	1(Max)			
496.	Should support anomaly detection without any threat intelligence in place by using its artificial intelligence, deep-learning, un supervised and supervised machine-learning capabilities.	Mandatory	1(Max)			
497.	Solution should have rich dashboard with on click visualization of the incidences, illegitimate traffic for realtime monitoring	Weightage	Yes-5 Marks(Max) No-0			

Total Marks				**183 Marks(Max)**			
Network Load Balancer(NLB), Global Site Load Balancer(GSLB) external Application Delivery Controller (ADC)							
Minimum Core Specifications: 16 Marks							
498.	CPU	24 Core	Mandatory	1(Max)			
499.	Storage	256 GB SSD	Mandatory	1(Max)			
500.	RAM	256GB	Mandatory	1(Max)			
501.	Throughput	Http requests per second: 2.6M Concurrent L4 Connections: 45M L7 throughput: 30Gbps SSL Transactions Per Second ECC 256-bit curve (RSA 2K Cert): 20K	Mandatory	1(Max)			
502.	Throughput Scalability (without any additional hardware)	Http requests per second: 4M Concurrent L4 Connections: 65M L7 throughput: 100Gbps SSL Transactions Per Second ECC 256-bit curve (RSA 2K Cert): 60K	Mandatory	1(Max)			
503.	Power on demand	Dual AC/DC supply with hot swappable units	Mandatory	1(Max)			
504.	Form Factor	1RU(Preferably) in standard 42U Rack	Mandatory	1(Max)			
505.	Ports	(4X40GE QSFP+ SR4 or 4X100GE SFP+ Ports) and (8X10GE SFP+ ports) SFP+/QSFP+ 1X1G Management port All ports should be fully populated	Mandatory	4X40GE QSFP+ SR4 - 1 Mark 4X100GE SFP+ Ports -2 Marks(Max)			
506.	Protocols	TLS1.2 and TLS1.3 Support with Hardware Acceleration (SSL Chips / Cards)	Mandatory	1(Max)			
507.	Virtual Instances	15, scalable to 20 with complete network & resource isolation	Mandatory	1(Max)			
508.	High Availability - HA	Both Active-Active & Active-Passive	Mandatory	1(Max)			
509.	Load Balancing Algorithms Support	LEAST CONNECTION, ROUND ROBIN, LEAST RESPONSE TIME, HASH Based, LEAST BANDWIDTH, LEAST PACKETS, SNMP Load etc.	Mandatory	1(Max)			
510.	Load Balancing Protocol support	TCP, UDP, FTP, HTTP, HTTPS, DNS (TCP and UDP), SIP , RTSP, RADIUS, SQL	Mandatory	1(Max)			
511.	Application Optimization	Compression, caching, connection multiplexing, SSL offloading, TCP optimizations, TCP Buffering	Mandatory	1(Max)			

512.	GSLB Algorithm Support	Round Robin, Least Connections, Least Response Time, Least Bandwidth, RTT, Proximity	Mandatory	1(Max)			
Key Requirements: 70 Marks							
513.	Supported Load Balancing types: SLB / LLB / GSLB		Mandatory	1(Max)			
514.	The ADC should support auth enforcement prior to allowing access to HTTP/HTTPS SLB application - LDAP RADIUS, SAML, Oauth, Client certificate authentication, Web API Callout		Weightage	Yes-2(Max) No-0 Marks			
515.	Dual Stack IPv4 and IPv6 Support		Mandatory	1(Max)			
516.	Damping Sudden Surge in traffic so it does not overwhelm the servers by tracking the number of connections to the server, and adjust the rate of new connections to the server		Mandatory	1(Max)			
517.	IP Reputation to detect and block requests from Malicious Sources (SPAM / BOTNETS / Anonymous Proxies / TOR etc.)		Weightage	Yes- 10 Marks(Max) No-0 Marks			
518.	The ADC shall be manageable by SSH , HTTP, HTTPS, API, Console		Mandatory	1(Max)			
519.	Centralized Management should be available for Reporting, Alarm, Configuration Management, SSL Certificate Management and Analytics		Mandatory	1(Max)			
520.	The ADC solution shall conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950		Mandatory	1(Max)			
521.	The ADC solution shall conform to EN 55022 Class A/B or EN 55032 Class A/B or CISPR22 Class A/B or CISPR32 Class A/B or CE Class A/B or FCC Class A/B		Mandatory	1(Max)			
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.		Mandatory	1(Max)			
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.		Mandatory	1(Max)			
524.	The solution must have server load balancing algorithms like (but not limited to) round robin, weighted round robin, least connection, Persistent IP, Hash IP, hash Cookie, consistent hash IP, shortest response, proximity, SNMP, SIP session ID, hash header, Observed, Predictive, least session, least connections, super HTTP, least latency, weighted round robin and TCL based script for customized algorithm etc.		Mandatory	1(Max)			
525.	The Load Balancer shall distribute traffic efficiently while ensuring high application availability. It shall monitor server health to determine that application servers are not only reachable but alive. If the Load Balancer detects issues, it shall automatically remove downed servers from the server pool and rebalance traffic among the remaining servers.		Mandatory	1(Max)			

526.	Load balancing capacity to add unlimited new back-end server as member of load-balancing group and prioritize the traffic to send new back-end servers. Also, it should have mechanism to remove the back-end server from pool by gracefully without hampering any remote user connection so that existing user communication must not be disconnected during maintenance or troubleshooting window which will help more application availability.	Mandatory	1(Max)			
527.	The Load Balancer shall improve the user's experience by increasing server response time. Shall support Caching web content that saves network bandwidth requirements and reduce loads on backend web servers.	Mandatory	1(Max)			
528.	The solution must have ICAP integration with other security devices for file vulnerability, virus, Trojan scanning during file submission with web-applications to improve security or equivalent or built-in AV	Mandatory	1(Max)			
529.	The solution must have script-based functions support for content inspection, traffic matching and monitoring of HTTP, XML, generic TCP. Load balancer should support Policies to customize new features in addition to existing feature/functions of load balancer	Mandatory	1(Max)			
530.	The Load Balancer Shall have full traffic control and be able to route requests to servers based on region, device, browser, or several other factors. This enables organization to deliver customized application responses to users.	Mandatory	1(Max)			
531.	The proposed solution must be able to perform TCP multiplexing and TCP optimization, SSL Offloading with SSL session & persistency mirroring, HTTP Compression, caching etc. in active-passive high-availability mode.	Weightage	Yes-5 Marks(Max) No-0			
532.	The solution should support High Availability for both TCP session mirroring and SSL session mirroring in full-proxy (Forward Proxy and Reverse Proxy) mode in Active-Standby HA Architecture.	Mandatory	1(Max)			
533.	The entire management solution must be capable to store all the logs (request, response parameters). The log database system must be separated and redundant so that if the central management module is down, the logs should not be missed.	Mandatory	1(Max)			
534.	The solution must allow the user to use a standard browser to access the management UI. Management system can be a physical or virtual appliance. In case of virtual appliance offering bidder must mention required hardware details.	Mandatory	1(Max)			
535.	The solution support role-based admin access with roles like no access, Guest, Operator, Application editor, Resource Administrator and Administrator.	Mandatory	1(Max)			
536.	Able to secure synchronize configurations, DNS configuration, and persistence to provide stateful-failover of DNS query	Mandatory	1(Max)			
537.	Able to auto sync setup and synchronization of multiple devices thus eliminating difficult hierarchical management common to DNS	Mandatory	1(Max)			

538.	Provides global high availability and reliability of applications across multiple sites and ensures application availability by tracking and managing inter-dependencies between applications.	Mandatory	1(Max)			
539.	Solution should have inbox or centralized management-CLI, GUI for policy configuration and verification	Mandatory	1(Max)			
540.	Supports DNS A, AAAA, A6, CNAME, DNAME, HINFO, KEY, MX, NS, NXT, PTR, SIG, SOA, SRV and TXR records	Mandatory	1(Max)			
541.	Supports static route table and optional dynamic routing such RIP, OSPF, IS-IS, BGP	Mandatory	1(Max)			
542.	Supports multiple firmware and firmware uploads without resetting device	Weightage	Yes-5 Marks(Max) No-0			
543.	Able to cache DNS responses	Mandatory	1(Max)			
544.	Able to provide flexibility in having deterministic probers which communicate with each node to determine (depending on the probe or monitor configured) its availability, status, proximity, or responsiveness.	Mandatory	1(Max)			
545.	Able to perform intelligent probing of your network resources to determine whether the resources are up or down. This allows you to specify which device probe specific servers for health and performance data.	Mandatory	1(Max)			
546.	Able to inform administrator of query stats of device groups in synchronization to improve visibility, management and troubleshooting of groups	Mandatory	1(Max)			
547.	Able to support composite monitors, such as M of N rule (e.g., need only 2 successes out of 3 monitors).	Mandatory	1(Max)			

548.	Able to support static and dynamic load-balancing algorithms such as: • Round robin • Global availability • LDNS persistence • Application availability • Geography • Virtual server capacity • Least connections • Packets per second • Round trip time • Hops • Packet completion rate • User-defined QoS • Dynamic ratio • LDNS • Ratio • Kilobytes per second • RADIUS accounting	Mandatory	1(Max)			
549.	Supports built-in GEO-Location database for accurate Geo load balancing. The default database shall provide geolocation data for IPv4 addresses at the continent, country, state, based on IP Address available. This also allows user to define how traffic is routed based on this information.	Mandatory	1(Max)			
550.	Support intelligent routing with load balancing geography-based distribution via programmatic control	Mandatory	1(Max)			
551.	Able to support mixed combinations of IPv6 and IPv4 virtual addresses and nodes resolving AAAA queries without requiring wholesale network and application upgrades. This provides DNS gateway and translation services for hybrid IPv6 and IPv4 solutions and manages IPv6 and IPv4 DNS servers in DNS64 environments.	Mandatory	1(Max)			
552.	Able to support application-centric monitoring, persist user connections across applications and data centers and be automatically routed to the appropriate data center or server, based on application state, ensuring that users are directed back to the same site regardless of their entry point.	Mandatory	1(Max)			
553.	GSLB Algorithm Support: Round Robin, Least Connections, Least Response Time, Least Bandwidth, RTT, Proximity	Mandatory	1(Max)			
554.	Able to propagate the desired persistence information to local DNS servers, reducing the required frequency of synchronizing back-end databases and maintain session integrity.	Mandatory	1(Max)			
555.	Supports DNS fallback in case GLSB decision is not available	Mandatory	1(Max)			

556.	Deliver high speed standard (non-GSLB) DNS query responses. Proposed DNS solution must be capable of 1000000 DNS response per second from day 1.	Mandatory	1(Max)			
557.	The OEM/Manufacturer should have ISO 9001, ISO 14001, and ISO 27001 Certification. Bidder must submit the OEM's certificates.	Mandatory	1(Max)			
558.	Respective bidder also needs to ensure that the final deployment of the Web & API application security solution is done based on the standards design guideline and best practices keeping in mind the data center compliance requirements and operational requirements.	Mandatory	1(Max)			
559.	Bidder has to ensure that the final deployment is done by the OEM certified resources to validate design standards and best practices.	Mandatory	1(Max)			
560.	Bidder must submit the required performance document and compliance reference document for the proposed solution.	Mandatory	1(Max)			
561.	Bidder must provide the detail compliance report with reference. The reference URL / information of RFP technical specification compliance should be publicly available, referenceable, and accessible document.	Mandatory	1(Max)			
562.	Manufacturer's warranty part number should be mentioned, minimum 5 (five) Full years' warranty for technical solution support with Patch & New Software Upgrade, RMA replacement should be provided for the proposed solution from the date of commissioning.	Mandatory	1(Max)			
563.	IP Reputation to detect and block requests from Malicious Sources such as SPAM / BOTNETS / Anonymous Proxies / TOR etc. including ipv4 and ipv6 traffic	Mandatory	1(Max)			
564.	All components of the solution should be capable of both Active-Active and Active Passive High Availability and the feature should be enabled from Day 1	Mandatory	1(Max)			
Total Marks			**86 Marks (Max)**			
Multi Factor Authenticator						
Minimum Core Specifications: 46 Marks						
565.	MFA solution should be hardware based or software based with underlying hardware infra and deployed on-premises	Mandatory	1(Max)			
566.	Proposed device should be able to provide MFA for Windows (10 & above), Mac, Linux, IOS(ver 10 and above), Android(ver 7 and above) OS and Database, etc. including their future versions.	Mandatory	1(Max)			
567.	Bidder should factor SSL Certificate wherever required.	Weightage	Yes-10 Marks(Max) No-0			

568.	Solution should be software token based and capable of generating synchronous token such as TOTP or HOTP, etc . Bidder has to provide Applications on all Android (7 and above), IOS(10 and above) including their future versions. The application must be present on Playstore/ Appstore and have a robust, comfortable interface.	Mandatory	1(Max)			
569.	MFA should have API for seamless integration with Bank's internal applications such as Active Directory, Microsoft O365, People soft HRMS , Swift Alliance, Windows Login, TACACS+, etc without any additional cost.	Mandatory	1(Max)			
570.	Sizing of the hardware and software should be considered for cratering atleast 1 Lakh users , application users	Mandatory	1(Max)			
571.	MFA app should be free from the latest OWASP top 10 vulnerabilities and should be free from all vulnerability at the time of deployment.	Weightage	Yes-10 Marks(Max) No-0			
572.	Proposed application should not be open sourced. Licensing, if any, should be for the entire period of the contract.	Mandatory	1(Max)			
573.	Proposed application should be a dedicated application for the Bank and Bank's logo should be integrated in the application. Bidder will be responsible for updating the application periodically, incorporating security fixes, making the application compatible with future versions of both the OS and maintenance of the application.	Mandatory	1(Max)			
574.	All components of the solution should be capable of both Active-Active and Active-Passive High Availability and the feature should be enabled from Day 1	Mandatory	1(Max)			
575.	Able to crater for atleast 1 Lakh users from day 1	Mandatory	5L and above Users-5 Marks(Max) Upto 4L Users Users-4 Marks Upto 3L Users Users-3 Marks Upto 2L Users Users-2 Marks Atleast 1L Users Users-1 Mark			
576.	Adaptive/ Risk based authentication capabilities	Mandatory	1(Max)			
577.	Support Open ID and SAML 2.0 natively and should be able to integrate with AD	Mandatory	1(Max)			
578.	Support failover to the authentication server at the DR site when the authentication server at primary site goes down	Mandatory	1(Max)			

579.	MFA solution should be able to integrate with any third-party application that support Radius, LDAP, SAML 2.0 or OIDC as authentication protocols, third party applications hosted in Bank for internal users as well as for customers as per the banks requirement	Mandatory	1(Max)			
580.	The agent should be dormant/idle when not performing any authentication activities	Mandatory	1(Max)			
581.	The proposed solution should provide embedded database	Mandatory	1(Max)			
582.	Solution should not have any conflict with existing or proposed infrastructure security solutions	Mandatory	1(Max)			
583.	Industry grade (AES-256) encryption should be used for data flow between Central server and clients	Mandatory	1(Max)			
584.	The proposed solution should have OAUTH compliant time based	Weightage	Yes-5 Marks(Max) No-0			
Total Marks			**46 Marks (Max)**			
TOTAL SCORE			**1000 (Max)**			

ANNEXURE-XII

PERFORMA OF INDICATIVE COMMERCIAL OFFER (REVISED)

RFP Reference: PROCUREMENT & MANAGEMENT OF CYBER SECURITY COMPONENT

Table-A(A): Procurement of Devices with 3-year warranty and its AMC

Amount in ₹

Sr No	Item	Make/ Model/ Part Number	Multiplication factor (A)	Procurement Cost with 3 year warranty		AMC Cost for Year 4 & 5 (5-10% of B1)		Total Cost= B2+C2
				Unit Cost (B1)	Total Cost (B2= A*B1)	Yearly Unit Cost (C1) % of B1	Total Cost (C2= A*C1*2 (years))	
1	Internet Router		4					
2	DDoS Preventive System with Perimeter protection and cloud mitigation		4					
2.1	Additional hardware module for upgradation to next 10GBPS of throughput for DDoS		1					
3	Perimeter NIPS with built-in SSL/TLS Decryptor		4					
4	NGFW Firewall with Anti-APT, Threat Emulator/NIPS, SSL/TLS Decryptor, SSL VPN		4					
4.1	Additional hardware module for upgradation to next 20GBPS of throughput for NGFW		1					
5	Application Delivery Controller(ADC) with Threat Intelligence Gateway and SSL/TLS Offloader		4					
5.1	Additional hardware module for upgradation to next 10GBPS of throughput for ADC		1					
6.1	WAF		4					
6.2	SSL Visibility/Orchestrator		4					
7	Perimeter Analytics- Network Detection and Response with Security Analytics		4					
7.1	Storage of 400 TB for NBAD		2					

7.2	Additional storage of 100TB for NBAD		1					
8	NLB,GSLB, DNS Security with ext-ADC		4					
9	Multi Factor Authentication		4					
TOTAL COST(A(A))								

Table-A(B): Procurement of Devices with 3-year warranty and it's AMC
(Quantity to be specified by the Bidder)

Sr No	Item	Make/ Model/ Part Number	Multiplication factor (A)*	Procurement Cost with 3 year warranty		AMC Cost for Year 4th & 5th (5-10% of B1)		Total Cost= B2+C2
				Unit Cost (B1)	Total Cost (B2= A*B1)	Yearly Unit Cost (C1) % of B1	Total Cost (C2= A*C1* 2 (years)	
1	Interconnect Switch		1*					
2	Server		1*					
3	OS, DB and Others		1*					
4	Network Rack, Other Components		1*					
TOTAL COST (A(B))								

***Note: Bidder has to mention the quantity in multiplication factor table for the proposed number of devices. In case Bidder fails to mention the quantity, default value of 1 will be taken. In case of default value, i.e, 1, Bidder will have to factor the actual number of devices required, at the total cost of unit price of the product.**

Table-B: License Cost and ATS

Sr No	Item	Make/ Model/ Part Number	Multiplication Factor (A)	License Cost (One Time)		ATS for Year 4 & 5 (10-20% of License Cost)		Total Cost= (B2+C2)
				Unit Cost (B1)	Total Cost= (B2= A*B1)	Yearly Unit Cost (C1= % of B1)	Total Cost= (C2= A*C1*2 (years))	
1	Anti DDoS protection with perimeter protection		4					
	(i) Annual subscription for threat intelligence Feed		1					
	(ii) Cloud Mitigation with bandwidth of 5 Gbps		2					
	(iii) Incremental bandwidth for cloud mitigation of 1Gbps each		1					
2	Perimeter NIPS		4					
3	Application Delivery Controller(ADC)		4					
	SSL/TLS Offloader/ Orchestrator		4					
	Anti BOT		4					
	Threat Intelligence		1					
4	Perimeter Firewall		4					
	(i)VPN Blade		4					
	(ii)VPN Blade User licenses		14000					
	(iii)Additional VPN Blade user licenses		1000					
	(iv) Botnet		4					
	(v) Anti-Malware Protection		4					
5	ADC with Threat Intelligence Gateway, SSL/TLS Offloader		4					
6.1	WAF		4					
6.2	SSL Visibility/ Orchestrator		4					
7	Network behaviour analysis detection and response with security analytics		4					

	Annual subscription for threat intelligence Feed		1					
8	NLB, GSLB, ext ADC with DNS Security		4					
9	MFA		4					
10	**Threat Intelligence license(console)**		**1**					
TOTAL COST(B)								

Note: Above licenses quantities have been factored for the entire solution.

Table-C: OTS Support for 5 years

Sr No	Item	Multiplication Factor (A)	Unit Cost (B)	Total Cost= A*B*5 (years)
1	L4 Resource	1		
2	L3 Resource	2		
3	L2 Resource	9		
4	L1 Resource	39		
TOTAL COST (C)				

Table-D: Implementation Cost - Onetime*

Sr No	Item	Make/ Model/ Part Number	Implementation Cost		
			Multiplication Factor (A)	Unit Cost (B)	Total Cost=A*B
1.	Internet Router		4		
2.	Interconnect Switch		1#		
3.	Network Load Balancer with DNS Protection		4		
4.	DDOS Preventive System with Perimeter protection		4		
5.	Perimeter Firewall with Anti-APT, Threat Emulator/NIPS, SSL/TLS Decryptor, SSL VPN		4		
6.	Perimeter NIPS with built-in SSL/TLS Decryptor		4		
7.	Application Delivery Controller(ADC), TLS/SSLOffloader/ Orchestrator, VPN Gateway,		4		

8.	WAF		4		
9.	Network Detection and Response with Security Analytics		4		
10.	Multi Factor Authentication		4		
11.	NLB with GSLB, external ADC and DNS Security		4		
12.	Onsite Professional services for customization, implementation and fine-tuning (**ITEM Number 3 to 11**)		1		
TOTAL (D)					

*__Note: Bidder has to provide installation, integration, customization of any additional module added to each of the items from Sl No. 1 to Sl No. 12 without any additional cost to the Bank during the contract period.__
__# Quantity 1 indicates all the quantities of the respective components factored by the Bank/Bidder.__

Sr.	Mandatory Items	Total Cost
1	Total of Table A(A)	
2	Total of Table A(B)	
3	Total of Table B	
4	Total of Table C	
5	Total of Table D	
Total of Table Cost (1+2+3+4+5)		

Notes:
1. The Price discovery discovered through RFP will be valid for the contract period of 5 years and an additional 2 years (in case the contract is extended at the discretion of the Bank.)

2. The rates quoted in commercial bid should be inclusive of all taxes and duties except GST. However, GST shall be paid to the bidder on actual basis at the rate applicable. The rate of applicable GST should be informed and charged separately in the invoice generated for supply of the product.
3. Any column left blank by the bidder will result in disqualification of the bid.
4. Price of Solution quoted should be inclusive of 3-year warranty with all licenses/subscriptions and OEM's premium support.
5. ATS/AMC will be applicable after expiry of warranty period of three years.
6. ATS/AMC should be quoted in the specified range only (in %).
7. The multiplication factor as mentioned in above table (Table A) is only indicative and for the purpose of deriving the Total Cost for determining the H1 bidder. The actual quantity of any item ordered may vary according to the requirement of the Bank. In addition to the initial Order placed, Bank may place subsequent orders for any item, if required, at any time during the contract period of 5 years, at the unit rate finalized after Reverse Auction.
8. Bank may place Orders as and when required during the entire contract period at the unit rates finalized after Reverse Auction.. The actual quantity of any item ordered may vary according to the requirement of the Bank.
9. Bank is not bound to place any minimum order for any item.
10. AMC cost will be between 5-10% of the base price for each component and ATS cost will be 10-20% of the License Cost. Incase the AMC and ATS is not quoted within their specified range, Bank will recalculate the same to the nearest value of their respective specified range.

Signature of Authorized Signatory
Name of Signatory:
Designation:
Date:
Place:
Email ID:
Mobile No:
Telephone No.:
Seal of Company:

ANNEXURE-XI(B)

SCORING METHODOLOGY

RFP Reference: PROCUREMENT & MANAGEMENT OF CYBER SECURITY COMPONENT

This evaluation will be carried out on a total score of 100 on the basis of the following evaluation parameters defined in this section. The evaluation methodology is further broken down into sub areas as under.

Existing				**Revised**		
TECHNICAL ASSESMENT CRITERIA (A)				**TECHNICAL ASSESMENT CRITERIA (A)**		
S.N.	**Criteria**	**Total Marks**		**S.N.**	**Criteria**	**Total Marks**
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.	5		**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
	(One mark for each implementation)	(Max)			(One mark for each implementation)	(Max)
2.	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		**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
	(For three years of experience 3 marks will be awarded. 1 mark will be awarded for every additional year of experience)	(Max)			(For three years of experience 3 marks will be awarded. 1 mark will be awarded for every additional year of experience)	(Max)
3.	Supply and installation of proposed solution/model for Next Generation Firewall (NGFW) with similar or higher throughput.	3		**3.**	**Implementation of proposed Next Generation Firewall (NGFW) with same or equivalent throughput in BFSI sector/RBI/Govt. Sector/PSU by the OEM in India**	**2**
	Yes-3 Marks No-0 Marks	(Max)			**Yes-2 Marks No-0 Marks**	**(Max)**
	(*Performance Certificate by organisation and P.O. to be shared.)				(*Performance Certificate by organisation and P.O. to be shared.)	
4.	Supply and Installation of proposed solution/model for network Intrusion Preventive System (NIPS) with similar or higher throughput and core specifications	3		**4.**	**Implementation of proposed Network Intrusion Preventive System (NIPS) with same or equivalent throughput in BFSI sector/RBI/Govt. Sector/PSU by the OEM in India**	**1**
	Yes-3 Marks No-0 Marks	(Max)			**Yes-1 Mark No-0 Mark**	**(Max)**
	(*Performance Certificate by organisation and P.O. to be shared.)				(*Performance Certificate by organisation and P.O. to be shared.)	

5.	Supply and Installation of proposed solution/model for NLB, GSLB, ADC with similar or higher throughput and core specifications.	3		**5.**	**Implementation of proposed NLB, GSLB, ADC with same or equivalent throughput in BFSI sector/RBI/Govt. Sector/PSU by the OEM in India**	**1**
	Yes-3 Marks No-0 Marks	(Max)			**Yes-1 Mark No-0 Mark**	**(Max)**
	(*Performance Certificate by organisation and PO to be shared.)				(*Performance Certificate by organisation and PO to be shared.)	
6.	Supply and Installation of proposed solution/model for Network Detection and Response (NDR) with similar or higher throughput and core specifications	3		**6.**	**Implementation of proposed Network Detection and Response (NDR) with same or equivalent throughput in BFSI sector/RBI/Govt. Sector/PSU by the OEM in India**	**2**
	Yes-3 Marks No-0 Marks.	(Max)			**Yes-2 Marks No-0 Marks**	**(Max)**
	(*Performance Certificate by organisation and PO to be shared.)				(*Performance Certificate by organisation and PO to be shared.)	
7.	Supply and Installation of proposed solution/model for ADC with Threat Intelligence and TLS/SSL Offloader with similar or higher throughput and core specifications	3		**7.**	**Implementation of proposed ADC with Threat Intelligence and TLS/SSL Offloader with same or equivalent throughput in BFSI sector/RBI/Govt. Sector/PSU by the OEM in India**	**2**
	Yes-3 Marks No-0 Marks	(Max)			**Yes-2 Mark No-0 Mark** (*Performance Certificate by organisation and PO to be shared.)	(Max)
8.	Supply and Installation of proposed solution/model for WAF with similar or higher throughput and core specifications	3		**8.**	**Implementation of proposed WAF with same or equivalent throughput in BFSI sector/RBI/Govt. Sector/PSU by the OEM in India**	**1**
	Yes-3 Marks No-0 Marks	(Max)			**Yes-1 Mark No-0 Mark** (*Performance Certificate by organisation and PO to be shared.)	(Max)
9.	Supply and Installation of proposed solution/model for Anti-DDoS with similar or higher throughput and core specifications	3		**9.**	**Implementation of proposed Anti-DDoS with same or equivalent throughput in BFSI sector/RBI/Govt. Sector/PSU by the OEM in India**	**1**
	Yes-3 Marks No-0 Marks	(Max)			**Yes-1 Mark No-0 Mark** (*Performance Certificate by organisation and PO to be shared.)	(Max)
10.	Technical & Functional Specification Compliance as per scoring sheet in Table of Technical Requirements	80		**10.**	Technical & Functional Specification Compliance as per scoring sheet in Table of Technical Requirements	**40**
	Note: Technical mark calculation is of Total 1000 marks. The Technical marks so obtained by the bidder will be converted to equivalent of 80..i.e Technical and Functional Marks=80X(Marks Obtained by Bidder/1000)	(Max)			Note: Technical mark calculation is of Total 1000 marks. The Technical marks so obtained by the bidder will be converted to equivalent of 40..i.e Technical and Functional Marks=40X(Marks Obtained by Bidder/1000)	**(Max)**
11.	Marks on resources experience –	5		**11.**	Marks on resources experience –	5 (Max)
	1. 1 marks for minimum 10 CCIE/CISSP in the organisation for experience of minimum 5 years.				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				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)	(Max)			(Undertaking along with duly Bio Data of onsite resource experience to be submitted. Employee should be on company payroll)	
12.	Technical Presentation with Product Demonstration on Proposed Solution by the Bidder: **Technical presentation** will be evaluated on the following parameters:	50 (Max)		**12.**	Technical Presentation with Product Demonstration on Proposed Solution by the Bidder: **Technical presentation** will be evaluated on the following parameters:	**30 (Max)**
	1. Design of Proposed Solution				1. Design of Proposed Solution	
	2. Resilience of proposed architecture, approach and methodology				2. Resilience of proposed architecture, approach and methodology	
	3. Future scalability				3. Future scalability	
	4. Security Aspects				4. Security Aspects	
	5. Interconnectivity between devices for achieving highest throughput.				5. Interconnectivity between devices for achieving highest throughput.	
	Product Demonstration: Demonstration of in-depth understanding of the proposed project's technical and functional requirements. Major Criteria for demonstration (but not limited to) are given as under:				**Product Demonstration:** Demonstration of in-depth understanding of the proposed project's technical and functional requirements. Major Criteria for demonstration (but not limited to) are given as under:	
	· Bidder's understanding on project scope.				· Bidder's understanding on project scope.	
	· Bidder's knowledge and experience to deliver vis-à-vis scope of the assignment.				· Bidder's knowledge and experience to deliver vis-à-vis scope of the assignment.	
	· Real-life throughput of each module after enabling all features (certified by external agency)				· Real-life throughput of each module after enabling all features (certified by external agency)	
	· Project timeline, delivery organization and solution architecture.				· Project timeline, delivery organization and solution architecture.	
	· Vetting of Proposed architecture design and recommendation of devices by Certified Professionals				· Vetting of Proposed architecture design and recommendation of devices by Certified Professionals	
	· Device being proposed, it's scalability, throughput, number of ports.				· Device being proposed, it's scalability, throughput, number of ports.	
	· Bidder's ability to provide crisp and clear answers with strong content to questions asked.				Bidder has to demonstrate the proposed interconnectivity between the devices to achieve maximum throughput	
					Bidder has to demonstrate SSL Offloader capabilities and functional capabilities and their output.	
					· Bidder has to demonstrate the ability of the proposed threat intelligence system in terms of providing the brief history	

					of random public IPs which will be provided by the Bank at the time of technical presentation, etc	
13.	CMMI Level of Bidder	10		**13.**	Proposed OEM for NGFW/NDR/NIPS must have experience in Cyber Threat Intelligence or Forensic Investigations related to Cyber Security across various countries (minimum experience in 5 countries)	**5 (Max)**
	Level 5- 10 Marks	(Max)			(Purchase/Work Order copy to be submitted)	
	Level 4- 8 Marks				Experience in atleast 5 countries – 2.5 Marks	
	Level 3- 6 Marks				Experience in atleast 6 and upto 8 countries – 4 Marks	
14.	Proposed OEM for NGFW/NDR/NIPS must have experience in Cyber Threat Intelligence or Forensic Investigations related to Cyber Security across various countries (minimum experience in 5 countries)	10			Experience in atleast 10 countries or more – 5 Marks	
	(Purchase/Work Order copy to be submitted)	(Max)				
	Experience in atleast 5 countries – 5 Marks					
	Experience in atleast 6 and upto 8 countries – 8 Marks					
	Experience in atleast 10 countries or more – 10 Marks					
15.	Proposed OEM for NGFW/NDR/NIPS must release at least 5 reports publicly in a year covering High-tech crimes by different Threat Actor groups and such report should mention the technical details of the attacks and TTPs	10			**Total Marks**	**100(Max)**
	(Purchase/Work Order copy to be submitted)	(Max)				
	10 and above published reports – 10 Marks					
16.	Bidder having own Computer Security Incident Response Teams(CSIRTs) accredited by a recognized external agency	4				
	If Yes -4 Marks	(Max)				
	If No- 0 marks					
Total Marks		**200(Max)**				

Justification for the changes: Changes done as per modification in various clauses in the RFP and to rationalize the scoring.

ANNEXURE - XIII

PERFORMA FOR INTEGRITY PACT

To,
The Asstt. General Manager,
IT Procurement Department, HO: ITD
Punjab National Bank,
……
New Delhi

Subject: Submission of Tender for the work……

Dear Sir,

I/We acknowledge that Punjab National Bank is committed to follow the principle of transparency equity and competitiveness as enumerated in the Integrity Agreement enclosed with the tender/bid document.

I/We agree that the Notice Inviting Tender (NIT) is an invitation to offer made on the condition that I/We will sign the enclosed integrity Agreement, which is an integral part of tender documents, failing which I/We will stand disqualified from the tendering process. I/We acknowledge that THE MAKING OF THE BID SHALL BE REGARDED AS AN UNCONDITIONAL AND ABSOLUTE ACCEPTANCE of this condition of the NIT.

I/We confirm acceptance and compliance with the Integrity Agreement in letter and spirit and further agree that execution of the said Integrity Agreement shall be separate and distinct from the main contract, which will come into existence when tender/bid is finally accepted by Punjab National Bank. I/We acknowledge and accept the duration of the Integrity Agreement, which shall be in the line with Article 6 of the enclosed Integrity Agreement.

I/We acknowledge that in the event of my/our failure to sign and accept the Integrity Agreement, while submitting the tender/bid, Punjab National Bank shall have unqualified, absolute and unfettered right to disqualify the tenderer/bidder and reject the tender/bid is accordance with terms and conditions of the tender/bid.

Yours faithfully

(Duly authorized signatory of the Bidder)

To be signed by the bidder and same signatory competent / authorized to sign the relevant contract on behalf of Punjab National Bank.

INTEGRITY AGREEMENT

Punjab National Bank, a body corporate constituted under the Banking Companies (Acquisition and Transfer of Undertaking) Act 1970 (Act no V of 1970) and having its Head Office at Plot no. 4, Sector 10, Dwarka, New Delhi 110075, hereinafter referred to as “The Principal”, which expression shall mean and include unless the context otherwise requires, its successors in office and assigns of the First Part.

And

M/s. _____having its registered office at _____ hereinafter referred to as “The Bidder/Contractor”, expression shall mean and include unless the context otherwise requires, successors and permitted assigns of the Second part.

Preamble

The Principal intends to award, under laid down organizational procedures, contract/s for…….. The Principal values full compliance with all relevant laws of the land, rules, regulations, economic use of resources and of fairness/transparency in its relations with its Bidder(s) and/or Contractor(s).

In order to achieve these goals, the Principal will appoint Independent External Monitors(IEMs) who will monitor the tender process and the execution of the contract for compliance with the principles mentioned above.

Section 1- Commitments of the Principal

The Principal commits itself to take all measures necessary to prevent corruption and to observe the following principles: -

1. No employee of the Principal, personally or through family members, will in connection with the tender for, or the execution of a contract, demand, take a promise for or accept, for self or third person, any material or immaterial benefit which the person is not legally entitled to.

2. The Principal will, during the tender process treat all Bidder(s) with equity and reason. The Principal will in particular, before and during the tender process, provide to all Bidder(s) the same information and will not provide to any Bidder(s) confidential/additional information through which the Bidder(s) could obtain an advantage in relation to the tender process or the contract execution.

3. The Principal will exclude from the process all known prejudiced person.

If the Principal obtains information on the conduct of any of its employees which is a criminal offence under the IPC/PC Act, or if there be a substantive suspicion in this regard, the Principal will inform the Chief Vigilance Officer and in addition can initiate disciplinary actions.

Section 2- Commitments of the Bidder(s) / Contractor(s)

The Bidder(s)/Contractor(s) commit themselves to take all measures necessary to prevent corruption during any stage of bid process/contract. The Bidder(s)/Contractor(s) commit themselves to observe the following principles during participation in the tender process and during the contract execution.

a. The Bidder(s)/Contractor(s) will not, directly or through any other person or firm, offer promise or give to any of the Principal's employees involved in the tender process or the execution of the contract or to any third person any material or the other benefit which he/she is not legally entitled to, in order to obtain in exchange any advantage of any kind whatsoever during the tender process or during the execution of the contract.

b. The Bidder(s)/Contractor(s) will not enter with other Bidders into any undisclosed agreement or understanding, whether formal or informal. This applies in particular to prices, specifications, certifications, subsidiary contracts, submission or non-submission of bids or any other actions to restrict competitiveness or to introduce cartelization in the bidding process.

c. The Bidder(s)/ Contractor(s) will not commit any offence under the relevant IPC/PC Act; further the Bidder(s)/Contractor(s) will not use improperly, for purposes of competition or personal gain, or pass on to others, any information or document provided by the Principal as part of the business relationship, regarding plans., technical proposal and business details, including information contained or transmitted electronically.

d. The Bidder(s)/Contractor(s) of foreign origin shall disclose the name and address of the Agents/representatives in India, if any, Similarly the Bidder(s)/Contractor(s) of Indian Nationality shall furnish the name and address of the foreign principals, if any. Further details as mentioned in the "Guidelines on Indian Agents of Foreign Suppliers" shall be disclosed by the Bidder(s)/Contractor(s). Further, as mentioned in the Guidelines all the payments made to the Indian agent/representative have to be in Indian Rupees only.

e. The Bidder(s)/Contractor(s) will, when presenting their bid, disclose any and all payments made, is committed to or intends to make to agents, brokers or any other intermediaries in connection with the award of the contract.

f. Bidder(s)/Contractor(s) who have signed the Integrity Pact shall not approach the Courts while representing the matter to IEMs and shall wait for their decision in the matter.

The Bidder(s)/Contractor(s) will not instigate third persons to commit offences outlined above or be an accessory to such offences.

Section-3 Disqualification from tender process and exclusion from future contracts.

If the Bidder(s)/Contractor(s) before award or during execution has committed a transgression through a violation of Section 2, above or in any other form such as to put their reliability or credibility in question, the Principal is entitled to disqualify the Bidder(s)/Contractor(s) from the tender process or take action as per the procedure mentioned in the "Guidelines on Banning of business dealings".

Section 4- Compensation for Damages

(1) If the Principal has disqualified the Bidder(s) from the tender process prior to the award according to Section 3, the Principal is entitled to demand and recover the damages equivalent to earnest Money Deposit/Bid Security.

(2) If the Principal has terminated the contract according to Section 3, or the Principal is entitled to terminate the contract according to Section 3, the Principal shall be entitled to demand and recover from the Contractor liquidated damages of the contract value or the amount equivalent to Performance Bank Guarantee.

Section 5- Previous transgression

(1) The Bidder declares that no previous transgression occurred in the last three years immediate before signing of this integrity pact with any other Company in any country conforming to the anti-corruption approach or with any Public Sector Enterprises or central/state government department in India that could justify his exclusion from the tender process.

(2) If the Bidder makes incorrect statement on this subject, he can be disqualified from the tender process or action can be taken as per the procedure mentioned in" Guidelines on Banning of business dealing".

Section 6- Equal treatment of all Bidders/Contractors/Subcontractors

In case of Sub-contracting, the Principal Contractor shall take the responsibility of the adoption of integrity Pact by the Sub-contractor.

(1) The Principal will enter into agreements with identical conditions as this one with all Bidders and Contractors.

(2) The Principal will disqualify from the tender process all the Bidders who do not sign this Pact or violate its provisions.

Section 7- Criminal charges against violating Bidder(s)/ Contractor(s)/ Subcontractor(s)

If the Principal obtains knowledge of conduct of a Bidder, Contractor or Sub contractor, or of an employee or a representative or an associate of a Bidder, Contractor or Subcontractor which constitutes corruption, or if the Principal has substantive suspicion in this regard, the Principal will inform the same to the Chief Vigilance Officer.

Section 8- Independent External Monitor

(1) The Principal appoints competent and credible Independent External Monitor (IEM) Shri. Deepak Anurag (IA & AS, retd.) (email ID: anuragd@cag.gov.in) (Mob no. 9810676339) & Dr. Sarat Kumar Acharya (Ex-CMD, NLC India Ltd.), (email ID: sarat777@rediffmail.com), (Mob no. 9442118060) for this Pact after approval by Central Vigilance Commission. The task of the Monitor is to review independently and objectively, whether and to what extent the parties comply with the obligations under the agreement.

(2) The Monitor is not subject to instructions by the representatives of the parties and performs his/her functions neutrally and independently. The Monitor would have access to all Contract documents, whenever required. It will be obligatory for him/her to treat the information and documents of the Bidders/Contractors as confidential. He/she reports to the Managing Director and CEO, Punjab National Bank.

(3) The Bidder(s)/Contractor(s) accepts that the Monitor has the right to access without restriction to all project documentation of the Principal including that provided by the Bidder(s)/ Contractor(s). The Bidder(s)/Contractor(s) will also grant the Monitor, upon his/her request and demonstration of a valid interest, unrestricted and unconditional access to their project documentation. The same is applicable to Sub-contractor.

(4) The Monitor is under contractual obligation to treat the information and documents of the Bidder(s)/Contractor(s)/Subcontractor(s) with confidentiality. The Monitor has also signed declarations on „Non-Disclosure of Confidential Information" and of „Absence of Conflict of Interest". In case of any conflict of interest arising at a later date, the IEM shall inform MD & CEO, Punjab National Bank and recues himself/herself from that case.

(5) The Principal will provide to the Monitor sufficient information about all meetings among the parties related to the Project provided such meetings could have an impact on the contractual relations between the Principal and Contractor. The parties offer to the Monitor the option to participate in such meetings.

(6) As soon as the Monitor notices, or believes to notice, a violation of this agreement, he/she will so inform the Management of the Principal and request the Management to discontinue or take corrective action, or to take other relevant action. The monitor can in this regard submit non-binding recommendations. Beyond this, the Monitor has no right to demand from the parties that they act in a specific manner, refrain from action or tolerate action.

(7) The Monitor will submit a written report to the MD & CEO, Punjab National Bank within 8 to 10 weeks from the date of reference or intimation to him by the Principal and, should the occasion arise, submit proposals for correcting problematic situations.

If the Monitor has reported to the MD& CEO, Punjab National Bank, a substantiated suspicion of an offence under relevant IPC/PC Act, and the MD & CEO, PNB has not, within the reasonable time taken visible action to proceed against such offence or reported it to the Chief Vigilance Officer, the Monitor may also transmit this information directly to the Central Vigilance Commissioner.

(8) The word **'Monitor'** would include both singular and plural.

Section 09- Pact Duration

This Pact begins when both parties have legally signed it. It expires for the Contractor 12 months after the last payment under the contract, and for all other Bidders 6 months after the contract has been awarded. Any violation of the same would entail disqualification of the bidders and exclusion future business dealings.

If any claim is made/lodged during this time, the same shall be binding and continue to be valid despite the lapse of this pact as specified above, unless it is discharged. determined by MD & CEO, PNB.

Section 10- Other provisions

1. This agreement is subject to Indian Law. Place of performance and jurisdiction is the "Place of award of work".
2. The actions stipulated in this Integrity Pact are without prejudice to any other legal action that may follow in accordance with the provisions of to the extant law in force relating to any civil or criminal proceedings.
3. Changes and supplements as well as termination notices need to be made in writing. Side agreements have not been made.
4. If the Contractor is a partnership or a consortium, this agreement must be signed by all partners or consortium members.
5. Should one or several provisions of this agreement turn out to be valid, the remainder of this agreement remains valid. In this case, the parties will strive to come to an agreement to their original intentions.
6. Issues like warranty/Guarantee etc. shall be outside the purview of IEMs.
7. In the event of any contradiction between the Integrity Pact and its Annexure, the Clause in the Integrity Pact will prevail.

(For & On behalf of the Principal)	(For & On behalf of Bidder/Contractor)
(Office Seal)	(Office Seal)

Place……. Date……..

Witness 1:	Witness 2:
(Name & Address)	(Name & Address)