6.2.2.91 GTP of Oracle License Renewal

(To be filled up and signed by the Manufacturer & Tenderer, otherwise the offer will not be acceptable)

Oracle License Renewal		
Item Description	**Requirement**	**Bidder Response**
Brand	To be mentioned by the bidder	
Model	To be mentioned by the bidder	
Country of origin	To be mentioned by bidder	
Country of Manufacturer	To be mentioned by the bidder	

[The Tenderer should complete all the columns as required]

Signature:
Name & Designation of tenderer

Duly authorised to sign the Tender for and on behalf of the Tenderer

Signature
Name and Designation of Manufacturer

6.2.2.92 GTP of File Sandboxing

(To be filled up and signed by the Manufacturer & Tenderer, otherwise the offer will not be acceptable)

File Sandboxing			
S/N	**Item Description**	**Requirement**	**Bidder Response**
1	Brand	To be mentioned by the bidder	
2	Model	To be mentioned by the bidder	
3	Country of origin	To be mentioned by bidder	
4	Country of Manufacturer	To be mentioned by the bidder	
5	Quantity	One	
6	General Requirements	Solution Type: Advanced AI-powered sandboxing platform for detecting zero-day and unknown threats.	
7		Deployment Options: On-premises appliance, virtual machine (VM), cloud-hosted, or public cloud (AWS, Azure, GCP) & Air-gapped networks support	
8		The sandboxing solution must demonstrate rapid file processing capabilities to ensure minimal latency in threat detection workflows. Median Processing Time: ≤ 5 seconds per file. Average Processing Time: ≤ 15 seconds per file.	
9		The system should maintain high efficiency while performing comprehensive threat analysis, ensuring that suspicious files are flagged accurately without compromising speed	
10		The solution must balance performance and security, providing real-time verdicts and inline blocking for detected threats	
11		The solutions should provides comprehensive file scanning capabilities across shared folders and upload portals, including SMB, NFS, public network shares, and cloud storage such as Microsoft OneDrive. By analyzing files in these locations, the solution shoild detects hidden malware early, helping prevent lateral movement and insider threats before they can propagate within the network	
12	Integration	The solution shoud be integrated with Network Firewall (NGFW), Endpoint Security (EDR/EPP), Application Security (WAF), Email Security & other Firewalls.	
13		Must integrate third-party integration via JSON API or ICAP.	
14		The solution must support passive traffic inspection via sniffing mode to identify and analyze files transmitted over multiple protocols no limited to HTTP, FTP, POP3, IMAP, SMTP, SMB	
15		The solution must support passive traffic inspection via Net Share Scan mode to identify and analyze files transmitted over multiple protocols vi FTP, sFTP, CIFs, NFS, OneDrive, AWS S3 Buckets, Azure Blob, and Google Cloud storage	

16	Hardware/VM Specifications	The proposed solution shall be dedicated OEM purpose build hardware	
17		CPU: Multi-core processors optimized for sandboxing.	
18		Memory: Minimum 48 GB RAM	
19		Storage: Minimum 900 GB SSD-based storage for high-speed analysis.	
20		Network Interfaces: Minimum 4 x 1GbE	
21	Performance & Scalability	VM Capacity: Support up to 14 VMs for scalability and flexibility.	
22		Supported VM Types: Local, cloud, and custom VMs with multiple OS options (Windows, Linux, etc.).	
23		Sandboxing Throughput (Files/Hr): Minimum 8K	
24		Dynamic Analysis Throughput (Files/Hr): Minimum 400	
25	Detection & Analysis	Analysis Techniques: Combination of static analysis, dynamic behavioral analysis, and AI/ML-based detection.	
26		Inline Blocking: Ability to block suspicious files in real-time during analysis.	
27		OS type Supported: Microsoft Windows 11/10/8.1/7, macOS, Linux, Android, and ICS systems	
28		File Types Supported: Executables, documents, archives, scripts, Android files, Linux files, MacOS, Web files and other common file formats.	
29	Security & Compliance	Should provides real-time threat intelligence updates from OEM threat Intel from day one.	
30		Compliance Frameworks: Must support PCI DSS v4.0, CMMC 2.0, EU NIS2, and similar mandates for advanced malware protection.	
31		Reporting: Detailed reports mapped to MITRE ATT&CK framework, including IOCs (STIX 2.0 compliant).	
32		IOC sharing in STIX 2.0 format for threat correlation.	
33	Management & Monitoring	The appliance shall support SSH, HTTP/HTTPS & console access	
34		The sandboxing solution must provide comprehensive monitoring and management of virtual machine environments used for threat analysis inside the sandboxing appliance	
35		Dashboard: Single-pane-of-glass view for SOC and IR teams.	
36		Incident Response: Built-in investigative tools (packet capture, tracer logs, malware screenshots).	
37		Automation: Automatic submission of suspicious files from integrated security devices and real-time sharing of threat intelligence.	
38		Must include integrated monitoring, reporting, and troubleshooting engine accessible through a web-based GUI	
39		Logs should be exportable to external log server.	
40	MAF	Bidder must be submitted Manufacturer Authorization form (MAF)	
41	Warranty	Bidder should propose hardware & software for 3 (three) years OEM warranty and RMA support.	
42	Manufacturer's part number	Bidder should submit BOQ of proposed device including the details part numbers and Manufacturer's Warranty part number.	

43	Licesne	Bidder must offer Advanced Sandbox subscriptions including Sandbox Engine, AI Engine/Model, File Query, Real-Time Anti-Phishing (RTAP), Threat Intelligence (IOC), Industrial Security (OT) with security services (Antivirus, IPS, Web Filtering) for three years	
44	Supporting Document	Bidder must submit the required performance document and compliance reference document for the proposed device.	
45	Installation, Testing and Commissioning	Bidder must carry out on site installation, testing and commissioning. In consultation with IT Department, bidder must configure appropriate security and administration related policies, must do integration with other related hardware/software required to make the Network Functional and shall provide respective documentation to IT Division.	

[The Tenderer should complete all the columns as required]

Signature: Signature

Name & Designation of tenderer Name and Designation of Manufacturer

Duly authorised to sign the Tender for and on behalf of the Tenderer

6.2.2.93 GTP of Secure Web Gateway

(To be filled up and signed by the Manufacturer & Tenderer, otherwise the offer will not be acceptable)

Technical Specification of Secure Web Gateway			
S/N	**Item**	**Requirements**	**Bidder Response**
1	Brand	To be mentioned by the bidder	
2	Model	To be mentioned by the bidder	
3	Country of Origin	To be mentioned by the bidder	
4	Form Factor	Appliance should not comsme more than 2U rack space and mounting kit should be included	
5	Quantity	1 (One)	
6	License Capacity	The solution should have 5,00 user licenses with minimum 10,000 proxy/UTM session and scale upto 5,000 users	
7	Industry Recommendations	The OEM must be Recognized as a Leader in Forrester Wave™ Zero Trust Edge Solution, Q3 2023 Report	
8		The OEM must be recognized as a Leader in the 2025 Gartner® Magic Quadrant™ for SASE Platforms	
9		The proposed solution should have minimum 3 (three) install based reference at Banking & Goverment sector in Bangladesh.	
10		The OEM must have local employee & office in Bankgladesh to get the prompt response	
11		The Appliance OEM must have its own threat intelligence analysis center and Must use the global footprint of security deployments more then 20 years for comprehensive cyber secuirty threat protection	
12	Platform Requirements	The platform must protects user against internet-borne attacks by incorporating multiple detection techniques such as web filtering, DNS filtering, data loss prevention, antivirus, intrusion prevention and advanced threat protection	
13	Architecture	The proposed product should be dedicated OEM appliance based with multicore processor	
14	High Availability	The platform should support active-active & active-backup high availability with session synchronization	
15	Interface	Must have minimum 2 x 1G Base-T ports from day one.	
16	Power Supply	Must have dual power supply from day one	
17	Memoery	Must have 16 GB Memory or higher memory	
18	Storage	Must have 4TB or higher Storage	
19	Deployment	Deployment in following topologies: - L2 bridge mode (inline) - L3 route mode (inline) - Explicit proxy (inline + out-of-path) - Transparent proxy (inline + out-of-path)	
20		Support IPSec, GRE and SSL-VPN tunneling for roaming users	
21	Protocol Support	The propose solution must be able to proxy SMTP, POP3, IMAP, FTP, MAPI, DNS, RTMP, CIFS protocol	
22	User Authentication	User authentication must support RADIUS, LDAP, TACACS+, SAML, Keberos	

23	SSL Content Scanning and Inspection	The proposed system shall have the ability intercept and inspect content of SSL encrypted traffic of HTTPS protocols without needing of third party solution	
24	Application Control	The proposed system shall have the ability to detect, log and take action against network traffic based on over 3,000 application signatures	
25		Must support Custom Application Signature	
26	IPS	Proxy must uses a combination of IPS signature as well as signature less engines to prevent intrusions.	
27		Configurable IPS filters to selectively implement signatures based on severity, target (client/server), protocol, OS and Application types.	
28		Configurable IPS filter-overrides that provides specific signature exclusions or variations based on source and destination addresses	
29	DLP	Should supporting DLP features to block or log sensitive data for day one	
30	Web Filtering	Web Filtering should be configurable on a scheduled basis (i.e. time of day)	
31		Must support blocking of malicious and suspicious domains and URLs	
32		Must support static blacklists and whitelists	
33	DNS Filtering	The Propose solution must be able to filter DNS query based on category and has the ability to block the DNS query	
34	Anti Malware Protection	Must support for on-box-Anti-Virus / Anti-malware protection	
35		Must support integration with cloud sandbox to detect advanced threats	
36	Content Analysis	Solution supports on-box real-time analysis of images in order to control content for Adult, Alcohol, Drugs, Extremism, Gore, Weapons, swim/underwear	
37	Caching/Acceleration Functionalities	Must be able to cache/accelerate video services At least: YouTube, Veoh, DailyMotion, Facebook Video.	
38		Must be able to cache/accelerate online software updates At least: Microsoft, Adobe, Apple	
39	Management	Must Support HTTPS-based Web Management	
40		Must support SSH-based including public-key authentication and web CLI Management	
41		Must support role based administration	
42		Must support Administrative authentication via local database, Radius, LDAP and TACACS+	
43	Logging, reporting and alerts	Must Support SNMP v2c and v3 Traps for Alarm Management	
44		Syslog support for administrative events	
45		Must provide reporting of bandwidth savings	
46		Must provide Web Filtering usage reporting	
47		Solution must have a Log viewer	
48		Centralized reporting for multiple devices using an external solution.	
49		The solution must allow add widget into the main dashboard for monitoring and alerting purpose.	
50	Warrenty	Bidder should propose hardware & software for 3 years OEM warranty and RMA support.	
51	Manufacturer's part number	Bidder should submit BOQ of proposed device including the details part numbers and Manufacturer's Warranty part	

		number.	
52	Licesne	Bidder should quote necessary security subscription for 3 years, that include: 24x7 Comprehensive Support, Firmware and General Upgrades, IPS,Antivirus, DLP, Advanced Malware Protection, Web Reputation/Score, Content Analysis/Filtering, Web Filtering, Credential Phishing Prevention, Application Control, Stateful Firewall, Sandbox Cloud, Web and Video Caching, Traffic Shaping/QoS Policy and WAN Optimization	
53	Installation, Testing and Commissioning	Bidder must carry out on site installation, testing and commissioning.	

[The Tenderer should complete all the columns as required]

Signature:
Name & Designation of tenderer

Signature
Name and Designation of Manufacturer

Duly authorised to sign the Tender for and on behalf of the Tenderer

6.2.2.94 GTP of NDR

(To be filled up and signed by the Manufacturer & Tenderer, otherwise the offer will not be acceptable)

Technical Specification of NDR			
S/N	Item	Requirement	Bidder Response
1	Brand	Any International Reputed Brand	
2	Country of Origin	To be mentioned by the bidder	
3	Model	To be mentioned by the bidder.	
4	Form Factor	Maximum 2U rack mountable	
5	Safely Certification	Must have FCC Part 15 Class A, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB certification	
6	Industry Recommendation	The OEM must be recognize as strong performer" in Forrester's latest Network Analysis and Visibility (NAV) Wave in 2023	
7		The OEM must be a member of Cyber Threat Alliance (CTA) which is a non-profit organization that is working to improve the cybersecurity of our global digital ecosystem by enabling near real-time, high-quality cyber threat information sharing among companies and organizations in the cybersecurity field	
8		The OEM must have local employee & office in Bankgladesh to get the prompt response	
9	Systems Architecture	The NDR solution should be dedicated hardware based to support upto 10GB NDR throughput and more than 120,000 file per hour Malware Analysis.	
10		The NDR appliance should have minimum 4 x 10G SFP+ with SFP+ module	
11		The NDR appliance should dedicated HA & Management ports	
12		The NDR appliance should have minimum 7 TB storage with RAID 10	
13		The NDR applinace should have dual AC power supply fully populated (within box) from day one	
14		The NDR solution should be able to detect and prevent advanced Malware, Zero-day attack, ransomware, Industroyer, Downloader and targeted Advanced Persistent Threat without relying on just Signature database.	
15		The proposed solution should be able to detect and prevent advanced Malware, Zero-day attack, ransomware, Industroyer, Downloader and targeted Advanced Persistent Threat without relying on just Signature database.	
16		Solution MUST have ability to integrate with NGFW and other products for quarantine/banned IP, and ability to quarantine depending on severity of event.	
17		Solution should support for SIEM log integration.	
18		Solution MUST support 3rd party API call upon threat detection	
19	Lateral Movement Detection	The NDR should support On-premise Learning to reduce false positives by analyzing an organization's specific traffic and adapting to newly disguised threats	

20		The NDR solution should have traffic learning to be based full packet analysis & should not rely on netflow/sflow. Flow data provide limited information & is not acceptable to create a strong ML Model	
21		The NDR solution should etect Network Anomalies not limited to Encrypted attacks (TLS) via JA3/JA3s, Weak Cipher and vulnerable protocol detections, Malicious web campaign detection, Network Attacks (intrusions), Botnet Attacks (both DNS and IP based), Malware sub-second verdict	
22	Breach Detection Capabilities	Ability to detect and name botnet detections, both DNS and IP based botnet	
23		Ability to profile traffic using ML and identify anomalies	
24		Ability to detect and name malicious web campaigns	
25		Ability to detect Network Intrusions	
26		Ability to detect weak cipher and vulnerable protocols	
27		Ability to differentiate different malware and attack types	
28		Virtual Analyst Capabilities to offload/assist SecOps in Breach Prevention. Please detailed.	
29		Ability to trace the Source of infection e.g. WannaCry	
30		Sub-second detection without running/executing file like sandbox analysis	
31		Solution must be capable of high performance network traffic analysis, 10Gps line rate sniffer rate and at least 120K+ files per hour	
32		Solution must be able to stop "patient-zero" i.e. ability to stop the first malware download (web) from host i.e. inline blocking	
33		Solution must have proven detection rate via 3rd party validation such as malware strike packs from traffic generators.	
34		Solution must provide MITRE ATT&CK view of attacks	
35		Solution must be able to classify different malware types (e.g. Banking Trojan) and by hosts (e.g. Host1 infected with Ransomware and Downloader)	
36		Solution must detect "fileless" malware as a category. Fileless is defined as no files planted on infected hosts, purely operate in memory/CPU instructions level.	
37		Mature AI that applies 5+ million malware features to achieve sub-second verdicts for day-one deployment with the capability to learn new features	
38		Scientifically analyze zero days including fileless threats and classifies them into 20+ malware attack scenarios Ex. Ransomware, Downloader, Password Stelaer etc	
39		Solution should able to trace and correlate source of malware events	
40		Solution may provide a big picture for threat analysis for forensic investigation	
41	Deployment Management Capabilities	Solution can be deployed in sniffer mode without sensors	
42		Solution has ability to be deployed in a 'offline/airgap' (i.e. no Internet) environment.	
43		Solution should support active-passive high availability mode	
44		Solution must have ICAP support	
45		Solution must support white list settings to filter trusted	

		hosts	
46		Solution must support REST API for automation, please list capabilities with API	
47	Logging & Reporting	Display attack in timeline format, showing source of attack	
48		IOC export with STIX v2 format	
49		Supports remote logging	
50	Systems Administration	Support Gui & Cli for adminstration & troubleshooting	
51		Supports 2 factor for administrative logon	
52		Supports LDAP/RADIUS remote admins	
53		Supports RBAC for administrative access	
54	Warranty	Bidder should propose hardware & software for 3 years OEM warranty and RMA support.	
55	Manufacturer's part number	Bidder should submit BOQ of proposed device including the details part numbers and Manufacturer's Warranty part number.	
56	License	Bidder should quote necessary security subscription for 3 years including Network Anomalies and zero day Malware Detection	
57	Installation, Testing and Commissioning	Bidder must carry out on site installation, testing and commissioning.	

[The Tenderer should complete all the columns as required]

Signature: Signature

Name & Designation of tenderer Name and Designation of Manufacturer

Duly authorised to sign the Tender for and on behalf of the Tenderer