6.2.2.83 GTP of Anti-DDoS

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

Technical Specification of Anti-DDoS			
S/N	**Item**	**Minimum Requirement**	**Bidder Response**
1	Brand	Internationally reputed Brand	
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 bidder	
5	3rd Party Certification	The OEM of the Proposed brand must have ISO 27001 certification	
6		The OEM of the Proposed brand must have FCC Class A, VCCI and CE compliance certification	
7	Enclosure Type	Rack Mountable, Chassis base	
8	Hardware Architecture and Requirement from day one	The equipment must have dual AC power supply from day one	
9		Inspection and prevention should be done in hardware	
10		None of the following settings, features, options and mitigation should have ANY impact on system data or packet rate performance to the maximum bps and pps rating stated in system or Marking documentation.	
11		Solution should 100% inspection of every passing packet in both directions	
12		The equipment must have 4 x 1G Copper and 4 x 1G SFP interface from day one.	
13		Bidder must supply (Four) 04 nos 1GE Multi-mode module with necessary patch cord from day one. The entire module must be same OEM original.	
14	Features	Solution must support up to 6 Gbps of total inspected throughput from day one	
15		Solution must support up to 7 Mpps of total inspected throughput from day one	
16		This system must inspect 100% of passing data packets at the smallest packet size to the stated Mpps throughput. System must not down-sample packets until attack is detected to preserve CPU usage.	
17		Latency must be lower than 60 microseconds	
18		SYN Flood Mitigation must support upto 5 Mpps	
19		The DDos appliance should support of TCP Connections minimum 3.5 million	
20		DNS Query Flood Source Validation and mitigation must be in excess of minimum 1.5M Qps	
21		Solution must support fully autonomous DDoS Mitigation response time of under 2 seconds.	
22		Performance should not be limited by any licensing system.	
23	Defense Functions and Actions	System must not use signatures, System must have methods of using behavioral and heuristic analysis that do not require signature subscriptions nor FCAP nor Regex manual entries.	
24		The system must allow protection parameters to be changed while a protection is running. Such change must not cause traffic interruption	
25		System must be able to compensate for unusually high-rate Sources such as CDNs and Enterprise firewalls without seeing	

		false positive attacks	
26		System must be able to automatically compensate for seasonality of key data traffic parameters over days and weeks of changes. Automatic adaptive threshold algorithms must be in place for key threshold parameters.	
27		System must simultaneously support 4000 protected subnet definitions from IPv4/32 and IPv6/128.	
28		The system must by option, be able to drop individual invalid packets at line rate (no Thresholds) for Layer 3 and 4 anomalies (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, 48 Invalid TCP Flag combinations, Invalid ACK Number) and provide statistics for the packets dropped from a single drop per 5-minute reporting period.	
29		Solution must monitor and mitigate traffic for all 256 Layer 3 IP Protocols, showing traffic rates and dropped packets by Protocol, automatically identifying and blocking up to 24 million Sources responsible for over-Threshld traffic or destination rate-limiting as required.	
30		System must be able to automatically detect and drop TCP, UDP and other Protocol Fragment Floods, identifying and blocking up to 24 million responsible Sources (depending on model) or destination rate-limiting as required.	
31		System must be able to automatically detect and block floods for all 65,536 ICMPv4 and ICMPv6 Types and Codes.	
32		System must be able to optionally block all non-valid ICMPv4 and ICMPv6 Type and Code combinations as anomalies.	
33		Solution must automatically and continuously monitor and mitigate traffic for all 65,536 TCP and UDP ports, showing traffic rates and dropped packets per Port, automatically identifying and blocking up to 24 million responsible Sources when under Port Flood attack or destination rate-limiting as required. Must not require regex signatures or other manual selection of ports for mitigation.	
34		Solution must automatically pair inbound and outbound traffic with ports 1-9999 so that it is easy to differentiate inbound attacks with no outbound responses from normal 2-way traffic to these "service ports"	
35		System must monitor, set Thresholds, mitigate and log/graph inbound attacks from UDP ports 1-9999 as UDP Reflected attack ports.	
36		The system must optionally limit number of simultaneous TCP connections on a per-Source basis	
37		The system must support the dropping of idle TCP sessions if client is idle for a configurable time period.	
38		System must be able to bypass the configured idle timeout for specific Sources.	
39		System must detect all 14 TCP Flag combinations that are State anomalies depending on current state of any session, while monitoring 24 million sessions. Incorrect flag packets must be dropped from the first packet (no thresholds) to the stated pps capacity of the system.	

40		System must optionally set a threshold under which invalid TCP State flags can be ignored and not dropped.	
41		System must optionally validate sequence number of every passing TCP packet.	
42		System must automatically detect attacks and validate sources for SYN floods to the protected subnets and per-Destination IP with separate learned thresholds for each, as well as a further separate threshold for blocking over-threshold SYN-per-Source floods for up to 24 million Sources.	
43		The system must enforce minimal request size over time for TCP, HTTP to prevent Slow attacks.	
44		System must automatically detect and block HTTP METHOD Floods for all 8 valid HTTP Methods (GET, HEAD, OPTIONS, TRACE, POST, PUT, DELETE, CONNECT) as well as total Methods per Source IP for up to 24 million Sources.	
45		System must optionally treat as anomalies, HTTP versions below 1.0 and invalid versions.	
46		System must optionally treat as anomalies, invalid HTTP Methods.	
47		System must be able to automatically monitor and mitigate sources sending excessive URL, Host, Referrer, Cookie and User Agent traffic.	
48		System must optionally be capable of sending server RSTs to free server connection table space when the server is subject to L7 floods, slow connection attacks and high Connection per Source Floods.	
49		System must prevent SSL renegotiation attacks.	
50		System must be able to ACL DNS Fragments and any or all 65,536 DNS Resource Record types.	
51		System must be able to detect and drop DNS Fragment Floods, identifying and blocking up to 24 million responsible Sources.	
52		System must support detection, Source validation and mitigation of DNS Query floods of all types.	
53		For systems installed where encrypted DNS or asymmetric traffic is in use, Thresholds must be available for all 16 DNS Response Codes for improved DNS Response Flood mitigation.	
54		System must support at least 11 different types of DNS rate and comparative parameters to provide full mitigation of various DNS attacks.	
55		System must mitigate on both UDP and TCP DNS transactions.	
56		The appliance must support a broad range of high-performance L3-L7 ACLs without manual Regex creation and these ACLs must be configurable via REST API. All ACLs, to the system limits of all ACLs combined must have no impact on line-rate bps and pps performance or latency of the appliance.	
57		System must be able to block any or all fragmented packets in TCP, UDP, other L3 Protocols, HTTP and/or DNS.	
58		System must support optional IP Reputation service offering updates of known-malicious IPs from a central research and reporting center.	
59		System must be able to block up to 500,000 domain/subdomain names with upload of these via text file from 3rd-party Indicators of Compromise lists.	

60		System must support optional Domain Reputation subscription service with up to 1 million blacklisted FQDNs/Subdomains regularly and automatically downloaded from a central research and reporting center.	
61		System must be able to optionally support multiple ACLS for TCP and UDP ports (single port to entire port range) and any number of the 256 Protocols (single Protocol to entire Protocol range)	
62		System must support multiple ACLs for any Packet of specific length or range of lengths and optionally modify that ACL to include IP type (v4/v6), Protocol, Fragment, TCP/UDP Port, ICMP Type/code to refine the ACL.	
63		System must be able to block any individual, range or all DNS Resource Records.	
64		System must be able to allow all/block some or block all/allow some by IPv4 country Geo-location.	
65	Deployment Mode and Reliability	Should support Wire/Hub Link down synchronization	
66		Should support fail-open/fail-close Power fail bypass mode	
67		Should support Asymmetric mode	
68		Should support Tap Mode	
69		It should support Hardware Bypass for Copper/Fibre Interfaces available on Unit.	
70		Bypass Interface should monitor the link to the attached DDoS appliance by sending a heartbeat packet to the appliance once every second. If the optical bypass switch does not receive the heartbeat back, it automatically switches network traffic to bypass the unresponsive DDoS appliance, even if the appliance is still receiving power. The optical bypass continues to send the heartbeat and restores the traffic through the DDoS appliance as soon as the link is restored.	
71		The device must support High-Availability pair configuration.	
72		In High-Availability mode, system must be capable of active-active mitigation if required, including operating on 2 different legs of Asymmetric traffic installations.	
73	Management , Reporting and Logging	The system must report every dropped packet from single-packet anomalies to multi-billion packet floods	
74		The system must be able to generate Summary and Detail reports of the TOP Attacks	
75		Reports must be configured at end-user option to report on-demand or at 5-minute, hourly, daily, weekdays or days-of-month schedule at specfic times as configured.	
76		Reports must be available based on a drop count threshold as configured by the customer.	
77		Any Reports must be stored locally and optionally emailed to selected recipients.	
78		Reports must be available in HTML, Word and PDF format.	
79		Attack and Event logs, Thresholds and Traffic Statistics must be exportable in CSV and/or PDF format.	
80		Attack Logs must be exportable via syslog to same-vendor and 3rd-party syslog servers, Analyzers and SIEM products.	
81		System must support complete SNMPv3 MIB with Traps for important system functions and all attack logging.	
82		The management platform must be accessible via a web-based interface and ideally with no need for additional client software	

83		Should support RADIUS, LDAP, and TACACS+ Authentication including 2FA	
84	Warranty & Support	Three (03) years software and support including comprehensive warranty with Replacement/repair.	
85		The OEM must have local employee & office in Bankgladesh to get the prompt response	
86	Installation & Commissioning	Installation, testing and commissioning with necessary accessories	
87	**License**	The license period shall have at least 03 years and will be calculated from the first day of system handover.	

[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

6.2.2.84 GTP of Web Application Firewall with LB

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

Web Application Firewall with LB			
S/N		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 the bidder	
4	Country of Manufacturer	To be mentioned by the bidder	
5	Enclosure Type:	1U Rack-mountable	
6	Compliance Certification	The system must inherit the following Compliance Certification: CE, FCC, RCM, VCCI, BSMI, UL, CB	
7	Quantity	02 (Two)	
8	Platform Requirements	Platform should provide application acceleration, reducing load on websites/Application and performing load balancing as well as other features (SSL offload, proxy/reverse proxy, content routing, L4/L7 firewalling and more). Platform also should provide application availbility to improve user experience by using multiple technique that used for business continuance and disaster recovery between miltiple sites.	
9	Solution Architecture	The solution must be hardware appliance-based solution and all the services like Server Load Balancer, Link load Balance, Global Server Load Balancing and Application Security should be on single OS.	
10		The solution shall provide native support for ZTNA to enforce role-based application access for Layer 7 HTTPS and TCPS virtual servers. Access must be governed by ZTNA policies that validate user identity, device posture, and contextual attributes before granting application-level permissions. The solution should integrate with endpoint security and identity management systems to dynamically apply ZTNA tags and posture checks	
11		ADC should support hardware based SSL acceleration.	
12	Interface	ADC should have minimum 8 x 10G SFP+ , 4 x 1G Cu and 4 x 1G SFP interface from day 1.	
13		Bidder should supply 4 x 10G SFP+ module for each appliance. All SFP module should be OEM original.	
14	Storage	ADC should have a minimum local storage of 200 GB	
15	Memory	ADC should have a minimum memory of 32 GB	
16	Power Supply	ADC should have dual power supply from day 1	
17	System Performance	·L4 throughput: 35 Gbps or more	
18		L4 connection per second : 1 Million or more	
19		L4 concurrent connections: 35 M or more	
20		L4 HTTP Request Per Second: 2.5 M or more	
21		L7 throughput: 25 Gbps or more	
22		L7 Request per second: 200,000 or more	
23		SSL CPS/TPS 2K keys : 30,000 or more	
24		SSL Encryption Throughput: 18 Gbps or more	
25		Compression Throughput: 18 Gbps or more	
26		Virtual ADC/ Routing Domain / Virtual Domain: 15 or more	
27	High Availability	Solutions should support active-active and active-backup high availability from day 1	

28		Solution should support network based failover for session mirroring, connection mirroring and heartbeat check	
29		Solutions should support full configuration and session sync.	
30	Networking	Should support Static NAT, Hide NAT, and Dynamic NAT for flexibility and scalability	
31		Support integration with SDN technology like Cisco ACI, Nutanix, OpenStack, and Ansible	
32		Should support NVGRE and VXLAN tunneling protocols to extend isolated network segments between servers for multi-tenant data center networks	
33		Shoud support Static, BGP, OSPF & Policy based routing	
34		Should have IPv6 Support for SLB, interfaces, routing, and firewalling	
35	Server Load Balancing & Application Optimization Features	The solution should supports layer4 and layer 7 load balancing for well-known protocols like HTTP, HTTPS, TCP , UDP, FTP, RADIUS, RDP, SIP, DNS and more	
36		Should have virtual service definition with inherited persistence, load balancing method, and pool members	
37		Should support Layer 4/7 application routing policy and server persistence	
38		Should support scripting for event-driven rules using predefined commands, variables, and operators for SLB, content rewrite, persistencey,and security	
39		The solution should supports the load balancing methods not limited to Round-Robin, Weighted Round-Robin, Least Connections, Fastest Response, URI, Host, Host Domain	
40		Solutions should provide application & server health checks for well-known protocols like ICMP, TCP, TCP_ECHO, HTTP, HTTPS etc.	
41		Solutions should maintain server persistency using Source-IP /Network, Hash Header, Cookie, RADIUS Attribute, SSL Session ID persistency options	
42		Solution should support content routing and rewrite content	
43		Solutions should support custom scripting for SLB and content rewriting	
44		The solution should supports one to one NAT, Source NAT (change source IP), DNAT (change destination IP) and Full NAT (change source & destination IP)	
45		The solution should support application (JavaScript,xml) and text (CSS, html, xml, custom plain) compression/decompression for web site acceleration	
46		Solutions should capable of doing SSL offloading towards clients and SSL re-encryption towards the real servers.	
47		Solution should support SSLv3, TLSv1.0, TLSv1.1, TLSv1.2, TLSv1.3	
48		Should supprot Layer 7 DNS load balancing, security, and caching	
49		Solution should support full SSL forward proxy to inspect outbound traffic	
50	Global Server Load Balancing	Solution should support load balancing of servers between different data centres	
51		The solution should support hardened DNS server that can be deployed as the authoritative name server	
52		Solutions should have availability to determined of virtual server health by real-time connectivity checking	
53		The solution should have persistence response for applications	

		transactions across multiple hosts.	
54		The solution should support dynamic proximity which is determined by application response time (RTT probes), least connections, or byte-per-second.	
55		Solution should support DNS-based load balancing of inbound traffic.	
56		Solutions should support all DNS queries like CANME, A record, AAAA record, MX record, CNAME record, NS record, TXT record, SRV record.	
57		Solution should support Response Rate Limit to keeps the authoritative DNS server from being used in amplifying reflection denial of service (DoS) attack.	
58		Solution should support DNS Security	
59		The solution should support DNS64 to allow the resolution of addresses from the IPv4 world by creating synthesized AAAA records for hosts where no AAAA record is available.	
60	Web Application Firewall & Security Features	The solutions should able to protects web server from the below types of attack: • Cross Site Scripting • SQL Injection • Generic Attacks • Known Exploits • Trojans • Information Disclosure • Bad Robot • Credit Card Detection • Application Attacks	
61		The solutions should offer Web Application Vulnerability Scanning with the following signatures types: • MIME Signatures • Message Signatures • Files Signatures • Context Signatures • Apps Signatures	
62		Solution should provide XML and SOAP detection and validation with the following cases: • XML Format Check • SOAP Format Check • XML Limit Check • WSDL Check • Schema Validation • XML XSS and SQLi Protection	
63		Solution should provide JSON detection and validation with the following cases: • JSON Format Check • JSON Limit Check • JSON XSS and SQLi Protection	
64		Solution should Data loss prevention (DLP) feature allows Web Application Firewall (WAF) to prevent information leaks, damage and loss.	

65		Solution should have the option to verify and enforce of the below HTTP Header objects • Maximum URI Length • Illegal Host Name • Illegal HTTP Version • Maximum Cookie Number in Request • Maximum Header Number in Request • Maximum Request Header Name Length • Maximum Request Header Value Length • Maximum URL Parameter Name Length • Maximum URL Parameter Value Length • Maximum Request Header Length • Maximum Request Body Length	
66		Solution should have the option to verify and enforce of the HTTP Method (CONNECT, DELETE, GET, HEAD, OPTIONS , POST, PUT, TRACE) objects	
67		Solution should provide full URL Protection	
68		The solution should be capable to provide XSS & SQL Injection Protection using URI Detection, Referer Detection, Cookie Detection and BODY Detection	
69		Solution should provide protection against bots attack	
70		Solution should have the ability to prevent, detect and restore web defacement with multiple protocols (FTP/SSH/Windows File Share) supported.	
71		Solution should have the ability to prevent, detect and restore Brute Force Attack according to the Host, URL Pattern, Login Failed Code, IP Access Limit	
72		Solution should have the ability to protect/secure cookie from leakage by enforcing Cookie encryption, Cookie sign and Max-Age on Cookie	
73		Solution should able to support multiple type (video, picture, texts, audio) file restriction using action-based file enforcing and file size restriction	
74		Solution should have network layer DDoS prevention technique using IP Fragmentation Protection, TCP SYN flood protection, TCP slow data flood protection policy.	
75		Solution should have application layer DDoS prevention technique using HTTP flood protection, HTTP Connection Limit, HTTP Access Flood.	
76		Solution should have L4 IP firewall policy to allows or denies traffic based on a source address, destination address, and service	
77		Solution should have Intrusion Prevention Service (IPS) to provides the latest defenses against stealthy network-level threats.	
78		Solution shhould support user tracking and authentication to provide accurate policies to prevent fraud.	
79		The solution should be capable of publishing web applications and offering backend SSO access	
80		Solution should support Two-Factor Authentication	
81		Should support GEO-IP based protection	
82	Log and Reporting Features	The solution should be able to locally store event (audit), alert & traffic information	
83		The solution should be able to send all log types above to an external syslog server	
84		Should have a Reporting Engine built-in	

85		Should support integration with renowned SIEM tools like Arcsight, Splunk, Qradar and others	
86		Log and reporting solution must support custom reporting as on-demand	
87		The solution should have a dashboard for data analytics where top "N" information is displayed	
88	Device Administration & Management	Should support VM/HW based central Maangement if required in future	
89		Should support HTTP/HTTPS/SSH in interface management	
90		Solution should have In-build diagnostic utilities	
91		Should support role based admin access.	
92		Device should suppot SNMP	
93	Industry Recommendation	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	
94		The OEM must have local employee & office in Bankgladesh to get the prompt response	
95		The proposed solution should have minimum 3 (three) install based reference in Bangladesh.	
96	Warrenty & Support	Bidder should propose hardware & software for 3 (three) years OEM warranty and RMA support.	
97	Manufacturer's part number	Bidder should submit BOQ of proposed device including the details part numbers and Manufacturer's Warranty part number.	
98	Licesne	Bidder must offer necessary security license & subscriptions that includes " Server Load Balance, Global Server Load Balance, IP Reputation and GeoIP, Advanced Malware Protection, Intrusion Prevention Service, WAF, Credential Stuffing Defense, Sandbox Cloud, DLP, Threat Analytics, Advanced Bot Protection " for three years	
99	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.	
100	**License**	The license period shall have at least 03 years and will be calculated from the first day of system handover.	

[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