
**GUJARAT INFORMATICS LIMITED**
Block No. 2, 2nd Floor, Karmayogi Bhavan,
Sector-10A, Gandhinagar 382 010

# Request for Proposal (RFP) for Supply, Installation, Testing and Commissioning (SITC) of Anti-DDoS Appliance Solution with Comprehensive Onsite Warranty for Gujarat Security Operations Center at Gujarat State Data Centre (GSDC), Gandhinagar

**DISCLAIMER**

GIL through this RFP invites proposals from reputed firms (hereafter referred as 'Bidders') which meets the evaluation criteria and can get on boarded to offer Anti DDoS Solution for Gujarat Security Operations Center (GSOC).

The information contained in this Request for Proposal (RFP) document or subsequently provided to Bidder(s), whether verbally or in documentary or any other form by or on behalf of the Gujarat Informatics Limited (GIL)/DST, Government of Gujarat or any of their employees or consultants, is provided to Bidder(s) on the terms and conditions set out in this RFP and such other terms and conditions subject to which such information is provided.

The purpose of this RFP is to provide interested parties with information that may be useful to them in eliciting their financial offers (the "Proposal") pursuant to this RFP. This RFP includes statements, which reflect various assumptions and assessments arrived at by the TENDERER, in relation to the RFP. Such assumptions, assessments and statements do not purport to contain all the information that each Bidder may require. This RFP may not be appropriate for all persons, and it is not possible for the TENDERER, its employees, or Consultants to consider the investment objectives, financial situation and particular need of each party who reads or uses this RFP. The assumptions, assessments, statements, and information contained in this RFP, may not be complete, accurate, adequate, or correct. Each Bidder should, therefore, conduct its own surveys and analysis and should check the accuracy, adequacy, correctness, reliability and completeness of the assumptions, assessments, statements, and information contained in this RFP and obtain independent advice from appropriate sources before filling up the RFP. Any deviation in the specification or proposed solutions will be deemed as incapability of the respective Agency and shall not be considered for final evaluation process.

Information provided in this document to the Bidder(s) is on a wide range of matters, some of which depends upon interpretation of law. The information given is not an exhaustive account of statutory requirements and should not be regarded as a complete or authoritative statement of law. The TENDERER accepts no responsibility for the accuracy or otherwise for any interpretation or opinion on law expressed herein.

TENDERER- its employees and advisors make no representation or warranty and shall have no liability to any person, including any Applicant or Bidder under any law, statute, rules or regulations or tort, principles

of restitution or unjust enrichment or otherwise for any loss, damages, cost or expense which may arise from or be incurred or suffered on account of anything contained in this RFP or otherwise, including the accuracy, adequacy, correctness, completeness, delay or reliability of the RFP and any assessment, assumption, statement or information contained therein or deemed to form part of this RFP or arising in any way during the Bidding process.

For interpretation of any clause in the RFP or Contract Agreement, the interpretation of the TENDERER shall be final and binding on the agency.

If the Bidder fails to complete the due performance of the contract in accordance with the specification and conditions of the offer document, the Purchaser reserves the right either to cancel the order or to recover a suitable amount as deemed reasonable as Penalty/Liquidated damage for non-performance.

**Definitions**

| | |
|---|---|
| Authorized Signatory | The bidder's representative (explicitly, implicitly, or through conduct) with the powers to commit the authorizing organization to a binding agreement. |
| Bid | "Bid" means the response to this document presented in Single Packet, Technical Cum Commercial Bid and Financial Bid, which are supplied with necessary documents and forms as given in Annexure, complete in all respect adhering to the instructions and spirit of this document. |
| Bidder | "Bidder" means any individual/proprietor/ partnership firm/ agency/ company/ responding to Request for Proposal and who submits Bid. |
| Contract | Means the contract of service entered between the User Department and the "Service Provider" for SITC of Anti-DDoS solution at Gujarat Security Operations Center (GSOC) with the entire documentation specified in the RFP. |
| Day | "Day" means a working day as per rules of User Department. |
| EMD | Earnest Money Deposit |
| DD | Demand Draft |
| Purchaser | User Department |
| TC | Tender Committee |
| PBG | Performance Bank Guarantee |
| Security Deposit (SD) | Amount of the Order Value deposited by the Bidder and retained till the successful completion of the project (as long as the bidder fulfils the contractual agreement). |
| RFP | "RFP" means the Request for Proposal |

| | |
|---|---|
| Consignee | “Consignee” shall mean User Department. |
| Client | User Department/User Department’s Client |

## 1. Purpose of this Document

This Request for Proposal (RFP) has been published for and on behalf of the Gujarat Security Operations Centre (GSOC), Directorate of ICT & e-Governance, Science & Technology Department (DST), GoG, to select Agency for supply, implementation, integration, operation, maintenance, and support of an Anti-DDoS Solution for protection of the Government of Gujarat's critical ICT infrastructure and online services against Distributed Denial of Service (DDoS) attacks.

Gujarat Informatics Limited (GIL), acting as the Bidding agency for the Government of Gujarat, hereby invites proposals from eligible bidders who meet the qualification criteria prescribed in this RFP and possess the requisite technical expertise, experience, and capabilities to deliver the required Anti-DDoS Solution and associated services in accordance with the requirements specified herein.

The selected bidder shall be responsible for providing the Anti-DDoS Solution, including all necessary hardware and its accessories, software, premium licenses, implementation services, integration, training, monitoring, technical support, and maintenance services during the contract period, as detailed in this RFP document.

This RFP is neither an offer nor an agreement and is issued solely for inviting competitive bids from interested and eligible bidders. The selection of the successful bidder shall be carried out through the process specified in this RFP, on behalf of GSOC/DST, GoG.

GIL reserves the right to amend, modify, supplement, or cancel this RFP, or to extend the bid submission deadline at any stage of the bidding process without assigning any reason. In such an event, all rights and obligations of GIL and the bidders shall thereafter be subject to the revised terms and timelines as notified by GIL.

### Instruction to the bidders for online bid submission

i. Tender documents are available only in electronic format which Bidders can download free of cost from the website https://gil.gujarat.gov.in and https://gem.gov.in/.

ii. The bids have been invited through GeM portal, i.e. the eligibility criteria, technical and financial stages shall be submitted online on the GeM portal https://gem.gov.in/.

iii. Interested and eligible Bidders are required to upload the eligibility related document in eligibility bid section, Technical related document in Technical bid section & Commercial Bid in Commercial bid section. The Technical & Commercial Bid must be uploaded to https://gem.gov.in/.

## Fact Sheet

| | | |
|---|---|---|
| | GIL Contact person | **General Manager (Networking)**<br>**E-mail:** dgmtech-gil@gujarat.gov.in, mgrhninfra1-gil@gujarat.gov.in<br>**Contact-079-232-52026/59227** |

**Note:**

1) The TENDERER reserves all the rights to cancel the process and reject any or all the proposals at any time.

## 2. Eligibility Criteria

| S/N | Eligibility Criteria | Attachments |
|---|---|---|
| 1. | The bidder should be a registered company (registered under Indian Companies Act, 1956 or Indian Companies Act, 2013)/LLP Act in India and must have 3 years of existence in India as on bid submission. | Copy of certificate of Incorporation/LLP Registration, PAN and GST registration Certificate. |
| 2. | The bidder should have an average turnover of Rs. 40 crores in the last three financial years as on bid submission date. | The copies of Audited Annual Accounts/Balance Sheet along with Profit & Loss Account and CA Certified Statement for last three financial years as on bid submission shall be attached along with the bid. UDIN number should available in CA certificate. |
| 3. | The OEM of the proposed solution should have a average turnover of Rs. 100 crores in the last three financial years as on bid submission date. | The copies of Audited Annual Accounts/Balance Sheet along with Profit & Loss Account and CA Certified Statement for last three financial years as on bid submission shall be attached along with the bid. UDIN number should available in CA certificate. |
| 4. | The bidder should have experience in Supply, Installation, Testing and Commissioning (SITC) of Anti-DDoS solution. The following work order value criteria must be met in the last three financial years as on bid submission date (any one option):<br>□ One work order having value of Rs. 16 Cr or | Details of such projects undertaken along with work order/purchase order copy/clients' on-going (along with client certificate)/ completion certification with the details w.r.t to the clause should be enclosed. |

| | | |
|---|---|---|
| | □ Two work order, each work order having value of Rs. 10 Cr or<br><br>□ Three work order, each work order having value of Rs. 08 Cr<br><br>All work orders / contracts should be in the name of the bidder | |
| **5.** | OEM Should have supplied Anti-DDoS solution having value of Rs. 50 cr. work order should be available in the last three financial years as on bid submission. | Details of such projects undertaken along with work order/purchase order copy/clients' on-going or completion certification with the details w.r.t to the clause should be enclosed. |
| **6.** | Bidder and OEM should not be debarred in last two years by any Ministry of the Government of India or by any State Government of India or any of the Government PSUs at the time of bidding. | Self-Declaration /Certificate/ affidavit mentioning that the Bidder is not debarred as per the clause. |
| **7.** | The bidder should be authorized by the OEMs of the proposed equipment/devices to bid for this tender.<br>AND<br>The Proposed solution should not be End of Support (EoS) for 5 years from the date of installation | MAF for Authorized partner. Self-declaration if the bidder is an OEM. |
| **8.** | The Bidder should have at least one office in Gujarat If the Bidder is not having any office in Gujarat, then bidder should submit a letter of undertaking to open the office in Gujarat within 45 days from the date of award. | The copy of Property tax bill/Electricity Bill/Telephone Bill/GST/CST should be enclosed. Registration/Lease agreement should be submitted as proof Or Undertaking Letter should be enclosed. |

**Note:**

1. **All the details and the supportive documents for the above-mentioned items should be uploaded in the bid.**
2. **Bidder's experience, bidder's turnover criteria will not be considered for the GeM bid; the bidder must match the eligibility criteria, experience, and bidder's turnover criteria, as mentioned in this document, and will be considered for evaluation.**

## 3. Pre-bid Meeting

- A prospective Bidder requiring any clarification of the bidding documents may seek clarifications by submitting queries on email Id: mgrhninfra1-gil@gujarat.gov.in, dgmTech-gil@gujarat.gov.in prior to the date of Pre-Bid Meeting. No bid queries would be entertained post completion of Pre-Bid Meeting.
- Tenderer will discuss the queries received from the interested bidders in the Pre-Bid Meeting and respond the clarifications by uploading on the website https://gil.gujarat.gov.in.
- No further or new clarification whatsoever shall be entertained after the Pre-Bid Meeting.
- The interested bidder should send the queries as per the following format:

| **Bidder's Request for Clarification** | | | |
|---|---|---|---|
| Name of Organization submitting Request | | Name & position of person submitting request: | Address of organization including phone, fax, email points of |
| S.No. | Bidding Document Reference (Clause /page) | Content of RFP requiring Clarification | Points of Clarification Required |
| 1 | | | |
| 2 | | | |

## 4. SCOPE OF WORK

### 4.1 Broad Scope

The scope of work covers end-to-end supply, delivery, installation, configuration, testing, commissioning, integration, and maintenance of hardware-based Anti-DDoS appliances including:

- Supply of Anti-DDoS hardware appliances with all necessary accessories, rack units, transceivers, and inter-connect cables
- Highest category OEM support (24x7x365). This should be visible on OEM portal and SI should submit evidence.
- Integration with SDC's existing network infrastructure: upstream routers, core switches, firewalls, load balancers
- Integration with SDC's SIEM solution for log forwarding (Syslog / CEF / LEEF format)
- BGP peering configuration with SDC's two (02) upstream ISPs for traffic diversion during volumetric attacks
- Network design document, HLD, LLD, and as-built documentation
- Acceptance Testing (UAT) and performance validation
- Knowledge Transfer (KT) and technical training for SDC's IT/security team
- 5-year comprehensive onsite warranty from Go-Live.

### 4.2 Detailed Scope

#### 4.2.1 Hardware Supply and Deployment

- Supply, rack, and stack of DDoS appliances in GoG’s State data centers
- Power redundancy: dual redundant hot-swappable PSUs
- Cabling, labeling, and physical installation as per SDC standards
- Optical fiber and copper cable requirements, SFP/QSFP transceivers
- Rack space requirement to be specified by bidder; SDC to provide rack space, power, and cooling apart from this to meet the solution requirement additional all things to be bear by bidder
- Bidders must include all required compute, storage, OS, database license and any other hardware, software licenses required for the solution to work.

#### 4.2.2 Network Integration

- Inline mode: appliance deployed in traffic path between Internet router and internal firewall/DMZ

- On-Demand / Out-of-Path Scrubbing: BGP diversion: traffic rerouted to appliance for scrubbing during detected attacks; clean traffic re-injected via GRE / IPIP tunnel or policy-based routing.
- BGP peering with minimum 2 upstream ISPs at DC for traffic diversion
- IP prefix advertisement and withdrawal automation during attack onset and clearance

#### 4.2.3 Configuration and Tuning

- Baseline traffic profiling and threshold setting for all protected IP ranges/subnets
- Policy configuration for all attack vectors as defined in Section 5
- Rate-limiting, ACL, blacklisting/whitelisting policy configuration
- Application-specific protection profiles (HTTP/S, DNS, SIP, SMTP)
- Custom attack signatures and geo-blocking configuration

#### 4.2.4 Training

- Minimum 3-day onsite technical training for SDC's IT/Security team (minimum 10 participants)
- SELECTED BIDDER to arrange hands-on, including but not limited to the following:
  - solution architecture, configuration, monitoring, troubleshooting, alert tuning
  - Case studies
  - Individual hands-on exercises (LAB)
  - Current trends
  - Detection techniques
  - Policy configuration
  - Best practices
  - Mitigation Strategies
  - Other related tool topics, etc.
- Training material (soft and hard copy) to be provided
- Certification or attestation of training to be issued by OEM

#### 4.2.5 Implementation/Operation

- The proposed solution should seamlessly integrate with existing network/security setup of GSDC.
- The SELECTED BIDDER must take all necessary precautions to prevent damage to any other equipment, structures, or setups during their work. If any tenderer’s property is damaged due to the SELECTED BIDDER's negligence or carelessness, the SELECTED BIDDER will be

held financially responsible and the cost of repairs or replacements for such damages will be charged to the SELECTED BIDDER.

- The SELECTED BIDDER must ensure that project adheres to the SLA specified timeline.
- Following the implementation of the solution, the tenderer will conduct an acceptance test before signing Go-Live certificate. This process includes:
  - The tenderer will evaluate the implemented solution for compliance and functionality.
  - If the solution does not meet the required specifications or has significant discrepancies:
    - The tenderer maintains the right to nullify the entire contract. Any amount paid at this point would be recovered from the PBG (Performance Bank Guarantee) In such a case, the SELECTED BIDDER must remove their equipment at their own expense and risk.
  - Acceptance testing arrangements:
    - The SELECTED BIDDER will be responsible for organizing the test at the designated sites.
    - Tenderer officials and/or appointed TPA will be present during the testing. The implementation process will officially be deemed complete only upon the execution of the Go-Live certificate, signed by both tenderer & the SELECTED BIDDER.
- OEM/ISV to assess and certify the implementation, hardening and configuration of the solution. Health check should be carried out by OEM every half -year and yearly complete assessment to ensure the quality of implementation and operations by OEM itself of CPU utilization, database activities, OS status, etc.
- The OEM shall generate regular reports (Daily/Weekly/Monthly) on health and performance of security devices and systems and share to SDC team & In case any performance bottlenecks are identified by the OEM/tenderer’s team suitable rectification steps/proper Support shall be provided till eradication of the issue.
- The SELECTED BIDDER to deploy their OEM certified manpower operations team on-site once implementation gets completed, for 5 years to ensure stabilization and smooth operation & maintenance of the solution. This service to be provided at no additional cost to the tenderer.

- During this period, in case the any of the resources go on leave/ stay absent, replacement resources having equivalent or more experience and qualification has to be arranged by the SELECTED BIDDER to ensure that regular functioning of the solution is not hampered.
- The SELECTED BIDDER shall provide half yearly HW maintenance services during the period of contract/warranty. Professionally qualified personnel who have expertise in the hardware and system software and application(s) supplied by the SELECTED BIDDER will provide these services and report. No additional payment will be made for the same.
- The SELECTED BIDDER shall also provide the following documents as part of the deliverables of the project.
    - Original manuals of all proposed hardware/software/applications
    - Standard Operating Procedures of Installation /
    - Configuration Documents
    - Troubleshooting Manual
    - Executive summary report for the project to the management Functional and operational requirements
    - Project design/plan document
    - Product description
    - Guidance for best practices
    - Implementation guidelines.
    - Business Continuity /archival/purging /back up Policies/procedures
    - User acceptance test plan
    - If any training materials
- SELECTED BIDDER has to provide premium support (Top rated support) from OEM for TAC and support related cases.
- When required, OEM should be able to enhance/ integrate the solution with new regulatory requirements on ongoing basis with minimal effort.
- During complex DDOS attacks, OEM/ISV will provide telephonic & onsite support if asked by the tenderer, without extra charges. For this, the OEM/ISV should have a 24x7x365 support from their respective contact centers, to log the calls.
- The contact center numbers should be provided to the tenderer along with the escalation matrix mentioning the contact person’s name, number, Mail ID and designation in the company.

- Data Privacy:
  - In Hybrid environment –
  - Data Location: The Service Provider shall ensure that all data is stored within India as per regulatory requirements. Compliance shall be ensured with Indian data privacy laws, including the Digital Personal Data Protection Act and other applicable directives such as the Data Privacy Act, Data Retention Directive etc.

## 5. TECHNICAL SPECIFICATIONS

The Anti-DDOS Appliance should be a standalone, dedicated hardware appliance-based solution for DDoS Detection and Mitigation, and NOT a part of Router, Firewall, UTM, Application Delivery Controller, Proxy based architecture or any Stateful Device.

### 5.1 Platform Architecture Requirements

| Sr. | Requirement | Specification |
|---|---|---|
| 1 | Hardware Architecture | Purpose-built DDoS mitigation appliance; NOT a general-purpose x86 COTS server repurposed for DDoS. Must have dedicated ASIC / NPU / FPGA for packet processing. |
| 2 | Processing Model | Stateless packet processing – the appliance must NOT maintain full session state tables for DDoS mitigation. Stateless processing ensures the appliance itself cannot be overwhelmed by state exhaustion attacks. |
| 3 | Throughput License Capacity | 100 Gbps |
| 4 | Inspection & Mitigation Throughput | 100 Gbps bidirectional inspection AND mitigation throughput (not inspection-only). Throughput must be guaranteed under full DDoS attack load. |
| 5 | DDoS Flood Attack Prevention Rate | Minimum 140 Mpps (Million Packets Per Second) for DDoS Flood Attack Prevention Rate |
| 6 | Maximum Concurrent Attack Sessions | Unlimited – no session state maintained per DDoS mitigation flow. Must handle unlimited concurrent attack connections.<br><br>Unlimited concurrent sessions for stateless volumetric mitigation, with dedicated state/connection tables available for L7 proxy challenges and authentication checks. |
| 7 | SSL/TLS Connection per Session | Minimum 100 KCPS |

| | | |
|---|---|---|
| **8** | Latency Impact on Clean Traffic | <= 80 µsec |
| **9** | Hybrid Scrubbing | Explicitly requires a hybrid model where an on-premise device communicates with an Two ISPs scrubbing center when thresholds are crossed. |
| **10** | Physical Hardware Specifics: | Specifically mandates 16 x 10 GigE bypass ports (LR or SR) fiber ports, and hot-swappable dual power supplies. |
| **11** | Network Interfaces | minimum 16 x 10GE/25GE SFP28 ports for management and monitoring. |
| **12** | Power Supply | Dual hot-swappable, load-sharing redundant AC power supplies (1+1). |
| **13** | Form Factor | 2U rackmount chassis; standard 19-inch rack compatible. |
| **14** | External Intelligent Bypass / Fail-Open | Integrated hardware bypass (fail-open) capability to prevent network outage in case of appliance failure; must support optical and copper bypass. Additional hardware required should be bring by the bidder if any. |
| **15** | Hardware Lifecycle | OEM to confirm hardware EOL (End-of-Life) / EOS (End-of-Support) date minimum 5 years beyond date of Final Acceptance Test. |

### 5.2 DDoS Attack Detection & Mitigation Capabilities

The appliance must detect and mitigate, at a minimum, all of the following attack categories. Bidder to confirm compliance for each:

#### 5.2.1 Volumetric / Flood Attacks

| Sr. | Attack Vector | Minimum Mitigation Requirement |
|---|---|---|
| **1** | UDP Flood (all port ranges, fragmented and non-fragmented) | Must drop at line rate at full 100 Gbps |
| **2** | ICMP / ICMPv6 Flood | Rate limiting and threshold-based drop |
| **3** | TCP SYN Flood | Stateless SYN authentication / SYN cookie without state tables |

| | | |
|---|---|---|
| 4 | TCP ACK / RST / FIN Flood | Behavioral analysis and rate-limiting |
| 5 | Reflection & Amplification: DNS, NTP, SSDP, Memcached, CLDAP, WS-DD, CoAP | Source validation and rate-based blocking |
| 6 | IP Fragment Attacks (Teardrop, Ping of Death, Smurf) | Fragment reassembly and anomaly detection |
| 7 | GRE Flood, ESP Flood, Protocol 41 Attacks | Protocol-level rate limiting |

### 5.2.2 Protocol Attacks

| Sr. | Attack Vector | Mitigation Method Required |
|---|---|---|
| 1 | TCP Session Exhaustion / State Exhaustion | Stateless challenge-response (without maintaining state on appliance) |
| 2 | HTTP/HTTPS GET / POST Flood (L7) | Behavioral fingerprinting, CAPTCHA challenge, rate limiting per source IP |
| 3 | DNS Query Flood (Recursive, NXDOMAIN, ANY) | DNS rate limiting Per IP / subnet, source rate thresholds, DNS challenge |
| 4 | DNS Amplification / DNS Water Torture | DNS response rate limiting (DNRRL), query type filtering |
| 5 | BGP / Routing Protocol Attacks | Control plane protection; BGP session rate limiting |
| 6 | SSL/TLS Exhaustion Attacks | Hardware TLS acceleration for inspection; TLS handshake rate limiting |
| 7 | Slowloris / Slow HTTP attacks | Connection timeout enforcement, HTTP header completeness check |

### 5.2.3 Application Layer (L7) Protection

| Sr. | Capability | Specification |
|---|---|---|
| 1 | HTTP/HTTPS DDoS Protection | Deep HTTP inspection, URL rate limiting, method filtering (GET/POST/HEAD), User-Agent filtering |
| 2 | SSL/TLS Decryption for DDoS | Hardware-accelerated TLS 1.2 and TLS 1.3 decryption for application-layer inspection; TLS inspection throughput Minimum 100 KCPS |
| 3 | DNS Protection | DNS rate limiting per source, DNSSEC support, malformed DNS drop, RD flag filtering, TTL manipulation detection |
| 4 | SIP / VoIP Protection | SIP INVITE flood, OPTIONS flood, REGISTER flood mitigation |
| 5 | API Protection | Rate limiting on REST/SOAP API endpoints; JSON/XML payload inspection |

### 5.3 Detection Engine Requirements

| Sr. | Detection Mechanism | Requirement |
|---|---|---|
| 1 | Behavioral Baseline Learning | Automatic traffic profiling and adaptive baseline generation per IP, subnet, protocol, and port. Must auto-learn normal traffic patterns without manual configuration. |
| 2 | Real-Time Attack Detection | Detection-to-mitigation time: maximum 18 seconds for automated signature activation; desirable ≤ 10 seconds. |
| 3 | Signature-Based Detection | Pre-built library of DDoS attack signatures; real-time signature updates from OEM threat intelligence feed (cloud-connected or offline update) at <=4-hour interval. |
| 4 | Anomaly Detection | Statistical and machine-learning based anomaly detection for zero-day DDoS vectors. |
| 5 | Threat Intelligence Integration | Integration with OEM's curated global threat intelligence cloud for IP reputation scoring and known bad actor feeds at <=4-hour interval. Must support offline feed updates for air-gapped environments.<br>Feed DDoS attacks, scanners, anonymous proxies, IoT botnets and web application attacks, DDoS attack vectors, DDoS attack signatures, readymade and customizable mitigation templates etc. |
| 6 | False Positive Rate | Bidder to demonstrate false positive rate of < 1% in reference deployments. |
| 7 | IPv4 and IPv6 Support | Full dual-stack DDoS mitigation for IPv4 and IPv6 traffic simultaneously at full rated throughput.<br>Full feature and performance parity for IPv4 and IPv6 protocols across all detection and mitigation engines |

### 5.4 Traffic Scrubbing & Mitigation Methods

| Sr. | Scrubbing Method | Requirement |
|---|---|---|
| 1 | Inline Scrubbing | Always-on inline mode: all inbound traffic inspected in real-time without diversion; clean traffic forwarded with minimal latency as per SLA. |

| | | |
|---|---|---|
| **2** | On-Demand / Out-of-Path Scrubbing | BGP diversion: traffic rerouted to appliance scrubbing center during detected attacks; clean traffic re-injected via GRE / IPIP tunnel or policy-based routing. |
| **3** | Surgical Mitigation | Granular per-flow mitigation capability: ability to drop attack flows while passing legitimate flows from same source IP; not blunt IP-block based. |
| **4** | Blackholing / RTBH | Remote Triggered Black Hole (RTBH) support via BGP for extreme volumetric events as last resort. |
| **5** | Rate Limiting | Granular rate limiting: per source IP, per destination IP, per subnet, per protocol, per port — independently configurable. |
| **6** | Geo-based Filtering | Country/region-based traffic filtering with country-level block/rate-limit capability. GeoIP database must be updated at minimum monthly. |
| **7** | ACL / Blacklist / Whitelist | Dynamic and static ACL support: blacklist and whitelist IP ranges, autonomous systems (AS numbers), and CIDR blocks. |

### 5.5 Management & Visibility Requirements

| Sr. | Management Feature | Requirement |
|---|---|---|
| **1** | Central Management System (CMS) | Unified management platform for all appliances. May be hardware appliance or virtual machine. CMS must reside on-premises within state data center (no mandatory cloud dependency for operation). |
| **3** | Real-Time Dashboard | Graphical real-time dashboard: traffic analytics, attack vectors, source countries, top targeted IPs, mitigation status, throughput utilization. |
| **4** | Alerting & Notifications | Email, SNMP trap, and Syslog-based alerts for attack detection, mitigation start/end, threshold breach, appliance health events. |
| **5** | Log Management | On-box or external log storage. Log fields: timestamp, source IP, destination IP, attack type, protocol, action, throughput. Log retention: minimum 90 days on-appliance; export for long-term SIEM storage. |

| | | |
|---|---|---|
| **6** | SIEM Integration | CEF / LEEF / Syslog format log export to SDC's existing SIEM platform. REST API for integration. |
| **8** | Out-of-Band Management | Dedicated out-of-band management port (minimum 1GE) for appliance management independent of data plane. |
| **9** | NetFlow / IPFIX / sFlow Export | Support NetFlow v9 / IPFIX / sFlow for traffic visibility to external flow collectors / analyzers. |
| **10** | Forensic Packet Capture | Full or sampled packet capture capability for forensic analysis during and after attacks; PCAP file export. |
| **11** | Policy Management & Application Profiles | The solution shall support the creation of granular, application-specific security profiles. The vendor must provide the capability to configure different mitigation thresholds and inspection policies for each application hosted in the data center. |
| **12** | Application-Level Bypass & Fail-Safe Mechanisms: | The solution must provide an 'Application-Level Bypass' functionality, allowing the administrator to exempt specific application traffic from mitigation engines in real-time without taking the entire appliance offline. Furthermore, the appliance must support 'Fail-to-Wire' (physical bypass) capabilities, ensuring that in the event of hardware or software failure, the network link remains operational (traffic is passed through without inspection). |

### 5.6 Reporting Requirements

| Sr. | Report Type | Requirement |
|---|---|---|
| **1** | Attack Reports | Per-attack report: attack start/end time, duration, peak BPS/PPS, attack vectors, source countries, targeted resources, mitigation action taken. |
| **2** | Traffic Trend Reports | Daily, weekly, monthly traffic summary; clean vs. attack traffic ratio; throughput utilization trends. |

| | | |
|---|---|---|
| **3** | Executive Summary Report | Monthly executive-level report: high-level attack summary, top threats, compliance status, SLA adherence. |
| **4** | Compliance/Audit Reports | Reports suitable for regulatory audit: ISO 27001, cybersecurity framework compliance posture. |
| **5** | Custom Reports | Ability to create custom reports with user-defined time periods, protected IPs, metrics and any other. |
| **6** | Report Export | Export to PDF, CSV, and XLSX formats. Scheduled auto-delivery via email. |
| **7** | SLA Reports | Must provide all relevant real-time system generated report mentioned in SLA. |

### 5.7 Compliance, Certifications & Standards

| Sr. | Certification / Standard | Status Required |
|---|---|---|
| **1** | Common Criteria (CC) EAL2+ or higher for the DDoS appliance | Mandatory – CCRA-recognized certificate to be submitted |
| **2** | UL / CE / FCC / BIS certification | Mandatory – applicable regulatory certification for India market |
| **3** | RoHS Compliance | Mandatory |
| **4** | ISO 9001:2015 – OEM Quality Management | Mandatory – OEM certificate to be submitted |
| **5** | ISO 27001:2022 – OEM Information Security | Desirable – OEM ISMS certificate |
| **6** | MTBF of Appliance | Minimum 100,000 hours MTBF for the hardware chassis |
| **7** | Operating Temperature | 0°C to 40°C; Humidity: 10% to 90% non-condensing |
| **8** | MeitY / GoI Compliance | Proposed solution must comply with Restriction of Procurement due to National Security grounds; the OEM country of origin must not be on the restricted list. |

**The deployed solution should be capable enough to address any type of DDOS attack including zero-day not limited to mentioned list**

## 6. TECHNICAL COMPLIANCE CHECKLIST (TO BE FILLED BY BIDDER)

Bidders must complete the following compliance table for each specification.

Non-submission or incomplete compliance table will result in bid rejection.

| Sr. | Specification Parameter | Required Value | Offered Value | (Yes/No) |
|---|---|---|---|---|
| | **SECTION A: HARDWARE PLATFORM** | | | |
| **A1** | Hardware-based stateless appliance (not COTS server) | Mandatory | | |
| **A2** | ASIC/NPU/FPGA hardware acceleration | Mandatory | | |
| **A3** | Throughput License Capacity | 100 Gbps | | |
| **A5** | Inspection and Mitigation Throughput | 100 Gbps | | |
| **A6** | Attack Prevention Rate | ≥ 140 Mpps | | |
| **A7** | Max Concurrent Attack Sessions | Unlimited | | |
| **A8** | SSL/TLS Connection per Session | Minimum 100 KCPS | | |
| **A9** | Latency on clean traffic | <= 80 µsec | | |
| **A10** | Network ports (10GE) | ≥ 16 x 10GE | | |
| **A11** | Hardware Bypass (Fail-Open) | Mandatory | | |
| **A12** | Redundant Hot-Swap PSU | 1+1 Redundant | | |
| | **SECTION B: ATTACK MITIGATION** | | | |
| **B1** | UDP / ICMP / TCP Flood mitigation | Mandatory | | |
| **B2** | DNS DDOS mitigation | Mandatory | | |
| **B3** | HTTP/S L7 DDoS mitigation | Mandatory | | |
| **B4** | TLS 1.2 and 1.3 Inspection | Mandatory | | |
| **B5** | Stateless SYN authentication (no state table) | Mandatory | | |
| **B6** | IP, Port, Geo Location etc based filtering | Mandatory | | |
| **B7** | RTBH via BGP | Mandatory | | |
| | **SECTION C: DETECTION & INTELLIGENCE** | | | |
| **C1** | Behavioral baseline / auto-learning | Mandatory | | |
| **C2** | Time to Mitigate (TTM) | ≤ 5 minutes | | |
| **C3** | Threat intelligence integration (OEM curated global feed) | Mandatory | | |

| | | | | |
|---|---|---|---|---|
| **C4** | IPv4 and IPv6 simultaneous support | Mandatory | | |
| | **SECTION D: MANAGEMENT & REPORTING** | | | |
| **D1** | On-premises Central Management System | Mandatory | | |
| **D2** | SIEM integration (Syslog / CEF / LEEF / REST API) | Mandatory | | |
| **D3** | NetFlow 9/ IPFIX / sFlow export | Mandatory | | |
| **D4** | Forensic packet capture (PCAP) | Mandatory | | |
| **D5** | Policy Management & Application Profiles | Mandatory | | |
| **D6** | Application-Level Bypass & Fail-Safe Mechanisms | Mandatory | | |
| | **SECTION E: CERTIFICATIONS** | | | |
| **E1** | Common Criteria EAL2+ or higher | Mandatory | | |
| **E2** | UL / CE / FCC / BIS certification | Mandatory | | |
| **E3** | RoHS Compliance | Mandatory | | |
| **E4** | ISO 9001:2015 – OEM Quality Management | Mandatory | | |
| **E5** | ISO 27001:2022 – OEM Information Security | Desirable | | |
| **E6** | MTBF ≥ 100,000 hours | Mandatory | | |

## 7. SERVICE LEVEL AGREEMENT (SLA)

### 7.1 Appliance Uptime & Availability

The vendor has to ensure adherence to time-schedules given in this RFP. Non-adherence will attract penalties.

| Priority | SLA Requirement | Penalty |
|---|---|---|
| **P1 – Critical** | Ack ≤ 1h, Resolution ≤ 4h | 3% of Quarterly charges beyond 4h per breach |
| **P2 – Major** | Ack ≤ 2h, Resolution ≤ 8h | 2% of Quarterly charges beyond 8h per breach |
| **P3 – Minor** | Ack ≤ 4h, Resolution ≤ 24h | 1% of Quarterly charges beyond 24h per breach |

Priority will be decided based on business impact by bidder.

| # | Parameter | SLA Target | Penalty |
|---|---|---|---|
| **1** | Solution Availability | ≥99.95% (Quarterly) (excluding planned downtime) | 5% quarterly charges per 0.50% drop per quarter |
| **2** | Attack Detection Time | ≤ 60 seconds | 3% quarterly charges per breach |
| **3** | Mitigation Start Time | ≤ 60 seconds | 3% quarterly charges per breach |
| **4** | Time to Mitigate (TTM) | ≤ 5 minutes | 5% quarterly charges per breach |
| **5** | False Positive Rate | ≤ 1% | 3% quarterly charges per incident |
| **6** | Attack Report Generation | ≤ 15 min after attack | 2% quarterly charges per delay |
| **7** | Monthly / Quarterly SLA Report | Submission till 7th date | 1% quarterly charges per day delay |
| **8** | Back-to-back OEM Support Commitment | 24x7x365 support | 5% of quarterly charges per missed SLA |
| **9** | Repair or Replacement of any component or hardware, software | Malfunctioning of appliances, hardware, hardware components accessories, systems software, or any products, the relevant | 0.5% of quarterly charges per hour of delay or part thereof. |

| | | | |
|---|---|---|---|
| | | defect should be attended immediately and rectified within 4 hours of the receipt/notice of the complaint. | |
| **10** | Hotfix, patch deployment, Threat and Vulnerability Mitigation | Delay in Hotfix, patch deployment, Vulnerability Mitigation beyond 7 working days | 0.5% of quarterly charges per week delay or part thereof |
| **11** | CPU/Memory Utilization | Continuous utilization ≥ 80% measure more than 60 minutes exclude DDoS attack time period | Mandatory solution upgrade without additional cost to maintain threshold value otherwise 5% of quarterly charges per incident |

PENALTY FOR DELAY IN DELIVERY OF SOLUTION and SERVICES

1. Delay in submission of HLD/LLD and Hardware delivery beyond 4 weeks
2. Delay in installation and configuration with baseline tuning beyond 8 weeks: 0.5% of Total Contract Value per week or part thereof (max 10%)
3. Delay in FAT beyond 11 weeks: 0.5% of Total Contract Value per week or part thereof (max 10%)
4. Delivery & installation and FAT penalties capped at 10% of total Contract Value
5. Quarterly penalties capped at 25% of quarterly charges.

PENALTIES FOR ONSITE SUPPORT

| SR | SLA Requirement | Penalty |
|---|---|---|
| **1** | Onsite personnel not present within 1 hour when required (beyond regular timing) | Rs. 1000/hour. |
| **2** | Vendor change of personnel without 45 days' notice | Rs. 25,000 per instance |
| **3** | Replacement not provided within 30 days (if Tenderer requests) | Rs. 2000 per day after 30 days |

| | | |
|---|---|---|
| **4** | Absence/Leave of onsite person without replacement | Rs. 5,000 per instance |

**ADDITIONAL DOCUMENT TO BE SUBMITTED:**

In the technical bid section of GeM, the bidder is required to upload following documents.

1. MAF, Brochure and OEM Compliance of the Offered product (yes/No only) on OEM Letterhead. Any other remarks not accepted.
2. Compliance of the SOW, SLA, and Payment terms etc as uploaded as part of the GeM Bid on bidder's letterhead.
3. Undertaking as per guidelines published by Ministry of Finance, Dept. of Expenditure, Public Procurement division dated 23.07.2020 in the given format by Bidder as well as OEM.

### 7.2 Facility Management Support (FMS)

- Dedicated onsite FMS engineer at DC during business hours (10:00 – 19:00 hrs) on working days, In case of leave/absence replacement must be provided with prior intimation.
- onsite FMS engineer have to present within 1 hour as and when required (beyond regular timing), This timing is indicative liable to vary as and when required without prior intimation.
- onsite FMS engineer responsibilities: Overall management, first-level troubleshooting, appliance health monitoring, log review, coordinate with OEM for P1/P2/P3 issues, annual OEM health check reports etc.
- onsite FMS engineer must hold OEM-level certification for the proposed product

## 8. ADDITIONAL COMMERCIAL & CONTRACTUAL REQUIREMENTS

### 8.1 Warranty and Comprehensive AMC

- 5-year Licenses, onsite comprehensive AMC from date of Go-Live: covers All License (Highest Available), hardware replacement, software updates/upgrades, and back-to-back premium (Highest Available) OEM support, by annual health check by OEM etc.
- All software upgrades, Hotfix and patches during warranty at no additional cost
- All type of feed (threat, signature etc) at no additional cost.
- Solution upgrade for any newly emerged threat/vulnerabilities must be provided without any additional cost.
- Replacement hardware in case of failure: within 4 hours for critical components (line cards, PSUs etc.)
- If significant failures occur in specific components during the contract period, the entire hardware unit must be replaced with a new one in a proactive manner without affecting daily operations.
- If Memory and CPU utilization exceeds 80% during the immediate post-deployment demonstration in a live environment, the equipment must be replaced with a higher-capacity unit at no additional cost.
- Any equipment found to have the wrong Bill of Materials (BoM), specifications, or feature sets must be replaced with equal or higher by the vendor at no extra cost.
- If supplied equipment is declared End of Sale during delivery, it must be replaced with hardware of equivalent or higher configuration at no additional cost.
- Should the hardware be declared EOL or EOS within Five years from FAT & Go-Live, the bidder or OEM is required to replace it with compatible, equivalent, or higher-configuration hardware at no extra cost.

### 8.2 Liquidated Damages (LD)

- Delay in delivery/commissioning beyond agreed Go-Live date: 0.5% of contract value per week of delay; maximum 10% of contract value
- Failure to meet SLA targets: LD to be computed as per deviation from agreed SLA thresholds
- LD recovery: Tenderer reserves the right to recover LD from Performance Bank Guarantee

### 8.3 Performance Bank Guarantee (PBG)

- PBG: 10% of total contract value, valid for contract period + 6 months
- PBG to be submitted within 15 days of issuance of Purchase Order
- Unconditional, irrevocable PBG from a scheduled commercial bank (other than successful bidder's bank)
- The Performance Guarantee shall be valid for a period of 180 days beyond Warrantee period and shall be denominated in Indian Rupees and shall be in the form of an unconditional Bank Guarantee issued by All Nationalized Bank including the public sector bank or Private Sector Banks or Commercial Banks or Co-Operative and Rural Banks (operating in India having branch at Ahmedabad/ Gandhinagar) as per the G.R. no. FD/MSM/e-file/4/2023/0057/DMO dated 21.04.2023 along with its earlier referenced GRs

  issued by Finance Department or further instruction issued by Finance department time to time in the format provided by GoG to be submitted within 15 days from the date of issue of work order/Letter of Intent. The Performance Guarantee shall be discharged by GoG and returned to the bidder within 30 days from the date of expiry of the Performance Bank Guarantee.

### 8.4 Delivery & Implementation Timeline

| Sr. | Milestone | Timeline (from PO Date) |
|---|---|---|
| **1** | Kick Off Meeting | Within 1 week |
| **2** | Submission of HLD / LLD / Implementation Plan,<br>Hardware delivery at DC | Within 2 - 4 weeks |
| **3** | Installation, cabling, racking at DC, Configuration, integration, and baseline tuning | Within 6 - 8 weeks |
| **4** | UAT and performance validation, Final Acceptance Test sign-off and SOP documentation and Go-Live | Within 10 -11 weeks |
| **5** | Onsite Training for team | Within 12 weeks |

**Payment Schedule**

| Sr. | Stage | Payment | Condition |
|---|---|---|---|
| **1** | Submission of HLD / LLD / Implementation Plan,<br>Hardware delivery at DC | 50% | hardware, software, licenses delivery |

| | | | |
|---|---|---|---|
| **2** | Installation, cabling, racking at DC, Configuration, integration, and baseline tuning | 30% | Installation, configuration, integration with existing solution |
| **3** | UAT and performance validation, Final Acceptance Test sign-off and SOP documentation and Go-Live | 20% | Final Acceptance test passed, SOP documentation & Training |
| **4** | Onsite Training for team, 5 years Comprehensive AMC, Warranty & Top Level OEM Support, O&M Charges | - | in 20 equal instalments at the end of every Quarter. |

**PRICE BID SCHEDULE:**

| Sr. No. | Description | Cost including GST (Rs.) |
|---|---|---|
| 1 | Capex-Cost of Anti DDoS solution<br>Inclusive of all the required hardware, Software and necessary Licenses required to make the solution fully functional.<br>As per the Scope of work, functional and technical requirement, including all cable & accessories, Installation, testing, commissioning, and training etc. | |
| | O&M Cost | |
| 1.1 | Propose solution - Cost for 1st year Comprehensive warranty and OEM Support | |
| 1.2 | Propose solution - Cost for 2nd year Comprehensive warranty and OEM Support | |
| 1.3 | Propose solution - Cost for 3rd year Comprehensive warranty and OEM Support | |
| 1.4 | Propose solution - Cost for 4th year Comprehensive warranty and OEM Support | |
| 1.5 | Propose solution - Cost for 5th year Comprehensive warranty and OEM Support | |
| Total cost (Rs.) | | |

Note:

- O&M cost should not be < 35% of total cost.
- L1 will be the lowest sum total of rates of all line items including GST as per GeM GTC.

**On letterhead of Bidder**

**Sub: Undertaking as per Office Memorandum No.: F. No.6/18/2019-PPD dated 23.07.2020 published by Ministry of Finance, Dept. of Expenditure, Public Procurement division**

**Ref: Bid Number: _____**

---

I have read the clause regarding restriction on procurement from a bidder of a country which shares a land border with India. I certify that we as a bidder and quoted product from following OEMs are not from such a country or, if from such a country, these quoted products OEM has been registered with competent authority. I hereby certify that these quoted product & its OEM fulfills all requirements in this regard and is eligible to be considered for procurement for Bid number_____.

| No. | Item Category | Quoted Make & Model |
|---|---|---|
| | | |
| | | |
| | | |

In case I'm supplying material from a country which shares a land border with India, I will provide evidence for valid registration by the competent authority, otherwise GIL/End user Dept. reserves the right to take legal action on us.

(Signature)
Authorized Signatory of **M/s <<Name of Company>>**

**On letterhead of OEM**

**Sub: Undertaking as per Office Memorandum No.: F. No.6/18/2019-PPD dated 23.07.2020 published by Ministry of Finance, Dept. of Expenditure, Public Procurement division**

**Ref: Bid Number: _____**

Dear Sir,

I have read the clause regarding restriction on procurement from a bidder of a country which shares a land border with India. I certify that our quoted product and our company are not from such a country, or if from such a country, our quoted product and our company have been registered with competent authority. I hereby certify that these quoted products and our company fulfills all requirements in this regard and is eligible to be considered for procurement for Bid number_____.

| No. | Item Category | Quoted Make & Model |
|---|---|---|
| | | |
| | | |
| | | |

In case I'm supplying material from a country which shares a land border with India, I will provide evidence for valid registration by the competent authority; otherwise, GIL/End user Dept. reserves the right to take legal action on us.

(Signature)
Authorized Signatory of **M/s <<Name of Company>>**