INDIAN INSTITUTE OF TECHNOLOGY BOMBAY
MATERIALS MANAGEMENT DIVISION
Powai, Mumbai 400076.

Ref No. (PR No. 1000039475) **RFQ. 3000013756**

Technical Specification for Procurement of 10 Gbps Anti-DDoS Solution

Sr No.	Item Description	Compliance (Yes/ No)
01	**1. Introduction** This document outlines the technical specifications for the acquisition of a 10 Gbps Anti-DDoS Solution by the Computer Centre, Indian Institute of Technology Bombay (IIT Bombay) as a Single Tender. **2. Key Features and Benefits** The proposed solution should offer the following features and benefits: • Comprehensive protection against all forms of DDoS attacks. • Provision of Clean Internet Pipe services to IIT Bombay. • Dedicated customer portal for monitoring threats and accessing traffic reports. • Assurance of secured internet services. • Optimization of network bandwidth. **4. DDoS Attack Types Covered** The solution should effectively mitigate various DDoS attack types including, but not limited to: • Chargen Amplification • DNS Amplification • MS SQL Amplification • Netbios • NTP Amplification	

- SNMP Amplification
- SSDP Amplification
- TCP SYN/ACK Amplification
- L2TP
- mDNS
- rpcbind
- TCP ACK
- TCP SYN flood
- TCP RST flood
- TCP NULL
- UDP flood
- ICMP flood
- IP Fragment
- IP Private
- IPv4 Protocol 0
- DNS flood
- RIPv1
- RIPv2
- HTTP/HTTPs Flood attack
- Ping of Death

5. Clean Internet Pipe Provisioning Process

The provisioning process for Clean Internet Pipe service should include the following steps:

- **Node In Charge:**
  - Submission of technical details via BMAP software.
  - Entry of customer information including public IP details, router interface details, etc.
  - Submission of work order in BMAP portal.
- **MPLS ANTI-DDOS Team:**
  - Configuration of managed routers on customer-connected PE router and Leader device.
  - Verification of managed routers.
  - Configuration of detection and mitigation templates.
  - Configuration of BGP community on routers.
  - Configuration of mitigation templates for customers.
  - Creation of customer portal user access login.

6. Service Assurance

The solution should ensure comprehensive service assurance through the following mechanisms:

- Detection: Generation of alerts based on predefined threshold values. Different alert levels trigger various actions by the NOC Anti-DDOS team.
- Mitigation: Manual mitigation steps initiated upon confirmation of a positive attack. Continuous monitoring and adjustment of mitigation parameters until attack traffic ceases.
- Customer Support: A full-fledged Security Operations Centre (ANTI-DDOS) must provide 24/7 customer support, including technical queries, alert information, mitigation information, and portal access issues.

7. Terms and Conditions

1. Payment will be made quarterly in arrears, after satisfactory report received from Indentor.

2. The minimum commitment period for service hiring will be one year.

3. Unsolicited bids will not be accepted.

Conclusion

The proposed Anti-DDoS solution from authorised vendor/ bidder should provide a robust defense against various DDoS attacks while ensuring the delivery of Clean Internet Pipe services to IIT Bombay. With comprehensive service assurance and customer support, this solution should aim to enhance the security and reliability of IIT Bombay's network infrastructure.