Guidelines for Mitigation of Distributed Denial of Service (DDoS) Attacks

Prepared by:
Cyber Security Directorate
Pakistan Telecommunication Authority (PTA)
Headquarters, Islamabad

Publication Year: 2026

Contents

Glossary / Definitions / Interpretations

1) **"Authority"** means the Pakistan Telecommunication Authority (PTA).
2) **"License"** means an authorization granted by the Authority for the establishment, operation or maintenance of any telecommunication system or the provision of any telecommunication service.
3) **"Licensee"** means the grantee or holder of a License issued by the Authority.
4) **"Denial of Service (DoS) Attack"** means a cyberattack in which a single source overwhelms a target system, network or application with excessive requests or traffic, rendering it unavailable to legitimate users.
5) **"Distributed Denial of Service (DDoS) Attack"** means a large-scale cyberattack launched simultaneously from multiple compromised systems (botnets) that flood a target with traffic, amplifying impact and complicating detection and mitigation efforts.
6) **"Botnet"** means a network of compromised computers, servers or IoT devices remotely controlled by an attacker to perform coordinated cyberattacks, including DDoS campaigns.
7) **"Scrubbing Center"** means a physical or virtual facility that inspects, filters and removes malicious network traffic while forwarding only legitimate traffic to its destination, ensuring the continuity of telecommunications services.
8) **"Out-of-Path Scrubbing"** means a mitigation mechanism that redirects network traffic to a separate scrubbing center during a DDoS attack, where malicious packets are filtered before the cleaned traffic is returned to the network.
9) **"Hybrid Architecture"** means a combined model of defense employing both on-premises and cloud-based mitigation solutions, integrated under centralized monitoring and threat intelligence sharing mechanisms.
10) **"BCP38"** means Network Ingress Filtering, as recommended by the IETF (RFC 2827), requiring network operators to block packets with illegitimate or spoofed source IP addresses to prevent DDoS and related attacks.
11) **"uRPF (Unicast Reverse Path Forwarding)"** means a network security technique that verifies the validity of the source IP address of incoming packets against the router's routing table, discarding packets with spoofed or non-reachable source IPs.
12) **"nTCERT"** means the National Telecom Computer Emergency Response Team, established as the sectoral CERT for Pakistan's telecommunications industry, responsible for cyber threat monitoring, incident coordination and information sharing.
13) **"nTSOC"** means the National Telecom Security Operations Center, a 24/7 operational arm of nTCERT responsible for continuous threat monitoring, analysis and visibility across critical telecom infrastructure.
14) **"GRE/BGP"** means Generic Routing Encapsulation and Border Gateway Protocol—technologies commonly used together to enable secure, efficient routing and

tunneling between diverse network environments or when connecting to cloud-based DDoS mitigation services.

15) **"Blackholing"** means a mitigation technique that drops all traffic destined for a targeted IP address or subnet to protect upstream and downstream networks from congestion during a DDoS attack.
16) **"Rate Limiting"** means a control mechanism that limits the number of requests or packets a server or device will accept from a given source over a specific period to mitigate flood-type attacks.
17) **"Mitigation Partner"** means an external service provider or international entity contracted by a Licensee to provide advanced DDoS mitigation services, such as global traffic scrubbing, filtering and real-time monitoring.
18) **"Traffic Anomaly Detection"** means a process or system used to identify deviations from normal network traffic patterns that may indicate the onset of a DDoS attack or other malicious activity.
19) **"Incident Response"** means a set of coordinated activities aimed at detecting, analyzing, mitigating and recovering from a cybersecurity incident, including DDoS attacks.
20) **"Resilience"** means the ability of a network, system or service to maintain acceptable levels of operation and quickly recover following a DDoS attack or similar disruption.
21) **"Threat Intelligence"** means information about existing or emerging threats, attack indicators and adversary tactics, techniques and procedures (TTPs) that can be used to detect, prevent and respond to DDoS attacks.
22) **"Telecommunication Service"** means a service consisting in the emission, conveyance, switching or reception of any intelligence within, or into, or from, Pakistan by any electrical, electromagnetic, electronic, optical or opto-electronic system, whether or not the intelligence is subjected to re-arrangement, computation or any other process in the course of the service;
23) **"Telecommunication System"** means any electrical, electromagnetic, electronic, optical or opto-electronic system for the emission, conveyance, switching or reception of any intelligence within, or into, or from, Pakistan, whether or not that intelligence is subjected to re-arrangement, computation or any other process in the course of operation of the system, and includes a cable transmission system, a cable television transmission system and terminal equipment;
24) **"Amplification Attack"** means a DDoS technique in which attackers exploit the response behavior of open or misconfigured servers (e.g., DNS, NTP, Memcached) to multiply attack traffic toward the target.
25) **"Reflection Attack"** means a DDoS technique in which an attacker sends forged requests to legitimate servers, which then send responses to the spoofed victim's IP address, overwhelming it with unsolicited traffic.
26) **"Layer 3/4 Attack"** means a DDoS attack targeting the network and transport layers (e.g., SYN flood, UDP flood, ICMP flood) to exhaust bandwidth or connection tables.

27) **"Layer 7 Attack"** means an application-layer DDoS attack (e.g., HTTP GET/POST floods) designed to exhaust server resources by mimicking legitimate user traffic.

28) **"Operational Controls"** means the technical, procedural and administrative safeguards implemented by a Licensee to detect, mitigate and respond to DDoS attacks in compliance with these Guidelines.

29) **"Incident Reporting"** means the formal process by which Licensees notify nTCERT and the Authority of any DDoS-related event, including its nature, scale, duration and impact, within the prescribed timeframe.

1 Introduction

The growing dependency on digital services and interconnected networks has amplified the impact of DDoS attacks worldwide. What were once isolated incidents of network congestion have evolved into sophisticated, multi-vector attacks capable of crippling national services, disrupting critical communications and eroding public trust.

In Pakistan, the telecommunications sector underpins digital transformation, e-governance, financial systems and national security operations. Consequently, maintaining uninterrupted service availability is a matter of national importance. These Guidelines provide a unified and proactive response framework to strengthen Pakistan's collective defense against DDoS threats.

These guidelines emphasize **collaboration**, **accountability** and **resilience**—ensuring that telecom licensees, ISPs, IXPs and national authorities operate in close coordination, supported by standardized detection, information-sharing and mitigation procedures. The overarching goal is to enhance operational readiness, reduce response times and foster a secure, resilient and trusted digital ecosystem in Pakistan.

2 Purpose

These DDoS Guidelines provide a clear, actionable framework to prevent, detect, mitigate and coordinate responses to Distributed Denial-of-Service (DDoS) attacks across Pakistan's telecommunications and internet ecosystem. The document aims to:

a. Set minimum operational and technical **best practices** for licensees;
b. Clarify roles and responsibilities for stakeholders including PTA, nTCERT and telecom operators; and
c. Define operational readiness measures and implementation roadmap so that the mitigation is standardized, timely, proportional and effective.

These Guidelines are developed to mitigate such risks by aligning with international frameworks and best practices from ENISA, GSMA, NIST, and IETF, as well as leading global CERTs, while tailoring them to Pakistan's specific operational and infrastructural environment to adopt a coordinated and standardized national anti-DDoS defensive posture.

3 Objectives

The key objectives of these Guidelines are to:

a. Strengthen national resilience against all kinds of DDoS attacks.
b. Establish a collaborative mitigation ecosystem integrating licensees' defenses, national scrubbing infrastructure and international overflow capacity where technically possible.

c. Enable **real-time threat intelligence exchange** through standardized telemetry and secure data interfaces.
d. Maintain operational readiness through periodic drills, testing and capability reviews.

4 Threat Landscape

4.1 Global Trends

Global DDoS attacks volume has exceeded ~30 Tbps (2025), driven by the proliferation of botnets, IoT exploitation, DDoS as a Service (DaaS), and cloud-based amplification. Increase in use of Over-the-Top (OTT) and Content Delivery Network (CDN) services demand hybrid detection capabilities spanning backbone, ISP perimeter and cloud edges. The global threat landscape continues to evolve toward multi-vector and AI-driven attacks, emphasizing the need for adaptive mitigation systems.

4.2 National Context

Pakistan's dependency on limited **submarine cable landing stations** and **Internet Exchange Points (IXPs)** heightens systemic exposure to large-scale DDoS disruptions. Major telecom operators have deployed anti-DDoS solutions, however, many of these solutions rely on legacy technologies and may not effectively address evolving attack techniques. There is a growing need to enhance these systems to ensure consistent and robust protection across networks.

Historical data shows that adversaries frequently leverage UDP-based amplification techniques—such as DNS, NTP, SNMP, Memcached, SSDP, CLDAP, and SMB—to disrupt network infrastructures.

5 Roles and Responsibilities Among Stakeholders

This section outlines the roles and responsibilities of all stakeholders to promote a collaborative approach in the detection, mitigation and response to DDoS attacks, thereby ensuring the continued availability and resilience of telecommunication systems and services.

5.1 Pakistan Telecommunication Authority (PTA)

Role: Regulate, monitoring, enforcement, compliance, Coordination, information sharing and operational support

Responsibilities:

a. Issue, maintain and periodically update these guidelines to ensure consistency and applicability across all stakeholders.

b. Ensure that all licensees implement and sustain effective DDoS detection, prevention and mitigation mechanisms.
c. Facilitate national-level coordination among licensees, the National CERT (NCERT) and other relevant entities during cyber incidents or whenever collaborative action is required.
d. Establish and enforce the necessary technical, operational and reporting standards pertaining to DDoS protection and mitigation.
e. Conduct regular audits and readiness evaluations to assess licensee capabilities and the overall national DDoS mitigation posture.
f. Maintain and manage centralized monitoring and coordination infrastructure to support response efforts during large-scale or cross-network attacks.
g. Aggregate, analyze and correlate reports received from licensees to detect and identify multi-operator or nationwide attack patterns.
h. Assist licensees during active mitigation by providing situational awareness, attack pattern analysis and by coordinating with upstream network providers as needed.
i. Disseminate early warning alerts, technical advisories and threat intelligence to all relevant stakeholders in a timely manner.
j. Lead national-level DDoS simulation exercises, compile post-incident analysis reports and promote capacity building through continuous training and awareness programs.

5.2 Licensees/Operators

Role: First-line Defense, Detection & Mitigation

Responsibilities:

a. **Mandatory Compliance**

1) Each Licensee shall ensure effective DDoS detection and mitigation mechanisms for both inbound and outbound traffic, either through in-house deployments or via upstream service providers, where visibility and enforcement are verifiable. Outbound DDoS risk shall primarily be mitigated through mandatory implementation of routing hygiene and anti-spoofing controls, including but not limited to BCP-38 / uRPF, MANRS principles, ingress and egress filtering, and securing customer edge devices (CPEs) in accordance with recognized security standards (e.g., ioXt Alliance guidelines or equivalent).

   Where implemented effectively, MANRS compliance at the ISP network level shall be deemed sufficient to meet baseline outbound DDoS mitigation requirements, subject to verification and audit.

2) Protection must cover all traffic categories, including enterprise, data center and service-specific segments.

3) Mandate security compliance requirements (e.g., ioXt certification or equivalent) for Customer Premises Equipment (CPE) vendors, to reduce botnet formation and amplification-based DDoS risks originating from insecure devices.
4) Timely reporting of any incidence of DDoS attack as per CTDISR.

b. **Layered Defense Strategy**

Each Licensees shall adopt a multi-layered defense approach to secure Internet-facing infrastructure: including but not limited to:

1) **Layers 3–4 (Network and Transport Layers)**
   a) Implement IP spoofing prevention using uRPF and BCP-38.
   b) Apply protocol-based rate limiting and implement traffic thresholds on critical interfaces.
   c) Deploy volumetric mitigation mechanisms such as BGP FlowSpec and Remote Triggered Black Hole (RTBH) filtering, and Access Control Lists (ACLs) to avoid or rapidly suppress attack traffic.

2) **Layer 7 (Application Layer)**
   a) Strengthen application-level defenses using Web Application Firewalls (WAFs), secure application proxies, and behavioral/anomaly-based analytics.
   b) Implement real-time detection and mitigation for HTTP, DNS, and API-targeted attacks, ensuring minimal service disruption.

c. **Telemetry and Threat Intelligence Sharing**
1) Licensees shall share summarized telemetry and security alerts with nTCERT/nTSOC in near real-time to support situational awareness and coordinated mitigation.
2) Integration must define:
   a) **Data Formats:** Net Flow/IPFIX, IOC feeds, STIX/TAXII, or equivalent.
   b) **Retention and Access:** Time limits, storage protections, and controlled retrieval.
   c) **Escalation Protocols:** Lawful access procedures for deep inspection and coordinated incident response.

d. **Routing and Network Hygiene**
1) Adopt **MANRS** principles for routing integrity, including prefix filtering, anti-spoofing, coordination, and global validation.
2) Implement **RPKI** to validate route origin announcements and prevent prefix hijacking.
3) Deploy passive defenses at international gateways and perimeter edges to filter invalid or malicious traffic before it enters domestic infrastructure, including:
   a) uRPF / BCP-38 for source IP spoofing prevention.
   b) Bogon filtering to block unallocated or reserved IP ranges.

c) Securing open DNS resolvers to prevent amplification attacks.
d) Basic protections at customer edges to prevent endpoints from being abused in attacks.

e. **Operational Readiness and Monitoring**
1) Maintain a **24×7 monitoring capability** with a clearly defined escalation process and designated contact points.
2) Execute mitigation promptly in accordance with **nTCERT advisories**.
3) Maintain **SLAs** with upstream or international mitigation partners to ensure scalable response capacity.

f. **Mitigation Tools and Automation**

1) Deploy mitigation and scrubbing capabilities at the network perimeter to neutralize impact on core network resources. Cloud based mitigation can complement on-premises defenses to address attacks closer to the source.
2) Leverage **AI/ML-based detection and response** technologies to accelerate identification and mitigation of AI-driven or large-scale attacks.
3) Establish robust contractual arrangements with cloud-based Anti-DDoS providers to guarantee sufficient clean bandwidth and mitigation capacity during high-volume scenarios.

g. **International Scrubbing / Vendor Contracts:** Ensure all agreements with international mitigation vendors include:
1) Data Protection Clauses compliant with domestic privacy laws, as applicable.
2) Jurisdictional Handling to keep data within approved or trusted regions.
3) Defined Escalation Paths for incident coordination involving foreign entities.

h. **Exercises and Readiness Assessment**
Participate in national-level exercises, drills, and readiness assessments to strengthen preparedness and response coordination.

5.2.1 International Mitigation Partners

Role: Provide extended or overflow mitigation capacity under SLA with the relevant licensee

Responsibilities:

a. Maintain 24×7 communication with the engaging licensee.
b. Provide attack analytics and post-incident reports to the concerned licensee and nTCERT as applicable.
c. Participate in testing and validation exercises with PTA and licensees.

5.3 Internet Gateways and Internet Exchange Points (IXPs)

Role: Enhance network resilience and provide collective visibility.

Responsibilities:

a. Provide aggregated or sampled traffic telemetry to nTCERT for early warning, trend analysis and threat detection, wherever technically feasible.
b. Promote and facilitate local peering arrangements among licensees to minimize reliance on international transit paths and enhance domestic traffic resilience.
c. Collaborate with nTCERT to host neutral monitoring, analytics or scrubbing infrastructure where feasible, supporting national-level visibility and mitigation capabilities.

6 Implementation Roadmap

6.1 Phase 1 – Foundation / Baseline Hardening

Timeline	*As per the prioritized roadmap of each licensee. However, must be implemented as soon as possible and not exceeding 6-months from the date of guideline issuance.*
Objective	To establish essential DDoS detection and blocking for all licensees and enforce baseline routing hygiene.
Mandatory Actions	a) Implement or confirm access to DDoS detection and blocking systems (either in-house or via upstream provider). b) Define and formalize incident escalation and response procedures. c) Establish SLAs with upstream and/or international mitigation partners for overflow protection. d) Nominate 24×7 security contact points for coordination with PTA and nTCERT.
Recommended Best Practices	a) Apply **BCP-38 / uRPF** for source-address validation to prevent spoofing. b) Adopt **MANRS** (Mutually Agreed Norms for Routing Security) for route integrity. c) Establish **traffic baselines** to support anomaly detection. d) Configure **rate limits, ACLs, and port filtering** on edge routers. e) Pre-configure **RTBH** and **BGP FlowSpec** for rapid mitigation activation.

	f) Centralize **logging and alerting** for early detection of traffic spikes. g) Conduct **staff training and readiness drills** to ensure operational competence.

6.2 Phase 2 – Operationalization

Timeline	*As per the prioritized roadmap of each licensee. However, must be implemented as soon as possible but not later than 12-months from the date of guideline issuance.*
Objective	Enable coordinated mitigation, routing integrity and real-time collaboration.
Mandatory Actions	a) Integrate DDoS detection and blocking systems with **automated alert sharing** to nTCERT. b) Participate in **joint tabletop and live simulation exercises** coordinated by nTCERT. c) Validate **response playbooks** and ensure escalation paths are tested and functional.
Recommended Best Practices	a) Deploy **scrubbing appliances** or virtual mitigation nodes where feasible. b) Implement **RPKI** and create **Route Origin Authorizations (ROAs)** to secure routing announcements. c) Automate **alert correlation and reporting dashboards** for improved visibility. d) Conduct **peer coordination tests** among ISPs and IXPs to validate end-to-end mitigation workflows.

6.3 Phase 3 – Centralized coordination and Improvement Planning

Timeline	*As per the prioritized roadmap of each licensee. However, must be implemented as soon as possible but not later than 18-months from the date of guideline issuance.*
Objective	Build centralized coordination and plan for national-level mitigation capacity
Mandatory Actions	a) Plan for the potential establishment of DDoS scrubbing and clearing-house mechanism linked with PTA nTCERT, subject to detailed technical, operational and economic feasibility assessments. b) Expand telemetry coverage to **IXPs, backbone interconnects, and high-risk segments**.

	c) Validate and standardize **escalation and data-exchange protocols** across all licensees. d) Conduct/participate in a **nationwide DDoS simulation exercise** to test interoperability and readiness. e) Start **telemetry sharing with nTCERT** f) Share **Indicators of Compromise (IOCs)** and incident data with nTCERT in near real-time. g) Participate in **regional anti-DDoS coalition networks** for cross-border information sharing.
Recommended Best Practices	a) Implement **automated telemetry collection** and IOC reporting tools for faster incident sharing. b) Enrich shared IOCs with contextual intelligence such as attack types and vectors. c) Conduct **joint drills with nCERT and sectoral CERTs and IXPs** to validate coordinated response where technically possible

6.4 Phase 4 – Continuous Enhancement

Objective	Sustain and strengthen national resilience through continuous assessment, learning, and capability enhancement.
Mandatory Actions	a) Conduct **annual audits, live drills, and post-incident reviews** to assess performance and lessons learned. b) Upgrade detection, analytics, and blocking capabilities to match evolving DDoS techniques. c) Review and update **SLAs and coordination protocols** based on threat evolution.
Recommended Best Practices	a) Implement **AI/ML-based adaptive detection systems** to enhance predictive capabilities. b) Develop a **continuous training and certification program** for relevant teams. c) Extend collaboration with **academic institutions, regional partners and cross-sector CERTs** for research and innovation.

7 Operational Readiness Requirements

Parameter	Target	Primary Measurement Method	Secondary Measurement Method

Detection Time	≤ 60 seconds	SOC/NOC logs, mitigation appliance	Reporting to PTA nTSOC/nTCERT where technically feasible and possible
Blocking Activation	≤ 120 seconds		
Full Mitigation	≤ 30 minutes		
Reporting to nTCERT	≤ 24 hours		
Latency Impact	≤ 150 ms average		

7.1 Operational Controls

a. Maintain continuously active detection and blocking systems.
b. Document response playbooks and escalation flows.
c. Ensure redundancy for detection and mitigation nodes.
d. Retain relevant telemetry for 90 days minimum.
e. nTCERT monitors aggregated data and issues coordination alerts.

References:

1. **CISA** - UNDERSTANDING AND RESPONDING TO DISTRIBUTED DENIAL-OF-SERVICE ATTACKS https://www.cisa.gov/sites/default/files/2024-03/understanding-and-responding-to-distributed-denial-of-service-attacks_508c.pdf *(Publication: March 21, 2024)*
2. **CERT EU** - DDoS Overview and Response Guide, https://cert.europa.eu/publications/security-guidance/CERT-EU_Security_Whitepaper_DDoS_17-003 *(Release Date: 03-06-2024)*
3. **Canadian Government** - Defending against distributed denial of service (DDoS) attacks – ITSM.80.110, https://www.cyber.gc.ca/en/guidance/defending-against-distributed-denial-service-ddos-attacks-itsm80110 *(February 2024)*
4. **APNIC** - Collaboratively increasing the DDoS resilience of digital societies through anti-DDoS Coalitions, https://blog.apnic.net/2024/05/14/collaboratively-increasing-the-ddos-resilience-of-digital-societies-through-anti-ddos-coalitions/ (*By Thijs van den Hout on 14 May 2024)*
5. **NCSC-UK** - DoS guidance,
6. **ISRAEL** - Preparation for Distributed Denial-of-Service (DDoS) Attacks, https://publications.iadb.org/en/publications/english/viewer/Preparation-for-Distributed-Denial-of-Service-DDoS-Attacks-Cybersecurity-Best-Practices.pdf *(October 2024)*
7. **EU CONCORDIA** - DDoS Clearing House Cook Book - https://www.concordia-h2020.eu/wp-content/uploads/2023/03/PREPRINT-D3-6_DDoS_Clearing_House_Cookbook.pdf (2022)
8. **NIST SP 800-189**: Resilient Inter-domain Traffic Exchange: BGP Security and DDoS Mitigation, *(December 2019)* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-189.pdf
9. How to prevent DDoS attacks, CloudFlare guide
10. AWS Best Practices for DDoS Resiliency, AWS guide
11. Azure DDoS Protection documentation, Azure documentation
12. Gartner DDoS Mitigation Solutions, Gartner