D

DDoS Attacks: Types, Detection, Mitigation, and Recovery

Learn how volumetric, protocol, and application-layer DDoS attacks differ, which metrics confirm an attack, and what to prepare before an incident.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
3 min

CONTENTS

In this guide

01 Main types of DDoS attacks
02 Reflection and amplification
03 Signs of a possible DDoS attack
04 Prepare before an attack
05 Mitigation during an attack
06 Why a local firewall may not be enough
07 DDoS vs. DoS and traffic spikes
08 How to recover from a DDoS attack

A **distributed denial-of-service (DDoS) attack** uses traffic or requests from multiple sources to exhaust a service, network, or supporting dependency. The objective is loss of availability, although attackers may also use disruption to distract defenders from

intrusion or fraud.

Not every outage is DDoS. Capacity failures, bad deployments, routing errors, certificate problems, and dependency outages can produce similar symptoms. Response starts by measuring where resources are failing.

01 Main types of DDoS attacks

- **Volumetric attacks** consume Internet bandwidth with very large traffic flows.
- **Protocol or state-exhaustion attacks** overwhelm firewalls, load balancers, connection tables, or network stacks.
- **Application-layer attacks** send requests that appear more like legitimate traffic but exhaust web, API, search, login, or database resources.
- **Multi-vector attacks** combine or switch techniques during the incident.

02 Reflection and amplification

An attacker can spoof the victim’s source address in requests to exposed UDP services. Those services send replies to the victim, reflecting traffic. When the reply is larger than the request, amplification increases the attack volume. Operators should prevent source-address spoofing and avoid exposing services that can be abused as amplifiers.

03 Signs of a possible DDoS attack

Look for abrupt traffic growth, bandwidth saturation, connection-table exhaustion, unusual geographic or network-source distribution, a surge in one request type, high cache misses, or rising latency and error rates. Compare edge, origin, DNS, load balancer, and application metrics. A healthy origin does not help if the upstream link is saturated.

04 Prepare before an attack

1. Map public services, dependencies, normal traffic, and capacity limits.
2. Arrange provider, hosting, CDN, DNS, and DDoS-mitigation contacts.
3. Deploy services behind scalable edge protection where appropriate.
4. Set rate limits, timeouts, caching, request-size limits, and health checks.
5. Protect origin addresses and restrict direct origin access.
6. Practice an incident runbook with communication and business-continuity steps.

05 Mitigation during an attack

Confirm the affected layer, engage upstream or scrubbing providers early, and apply targeted filters or challenges. Cache safe content and shed nonessential expensive functions. Preserve access for administrators through a separate path. Avoid broad blocks that harm more legitimate users than the attack, and monitor whether attackers change vectors.

06 Why a local firewall may not be enough

If malicious traffic has already filled the Internet connection, dropping it at the server is too late. Upstream filtering, anycast capacity, a CDN, or a specialist scrubbing service can remove traffic before the constrained link. Application-layer attacks still require application context and careful rate controls.

07 DDoS vs. DoS and traffic spikes

A denial-of-service attack can originate from one source; DDoS uses distributed sources. A legitimate flash crowd can also overload a service. Intent may be unclear initially, so engineering should focus on availability and measurable request behavior while security investigates source coordination and other malicious activity.

08 How to recover from a DDoS attack

Remove emergency rules carefully, verify data and authentication integrity, and review whether another incident occurred during the distraction. Preserve traffic samples and timelines, calculate user and business impact, tune thresholds, and update provider procedures. Do not expose a previously hidden origin as a quick workaround without access controls.

Recovery is complete only when normal capacity and routing are stable, temporary filters are documented or removed, monitoring thresholds are restored, and the origin is protected against direct access. Confirm with providers which attack vectors they observed and update the runbook before the next event.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com