DDoS attack playbook

Edition 16 November 2026. Free to copy and adapt under CC BY 4.0. Fields in [square brackets] are for you to fill in.

When to use this playbook

Use this playbook when a website, application or network service becomes slow or unavailable because of a flood of traffic or requests.

Before you start: prerequisites

Complete these before an incident, as part of planning.

- Normal traffic baselines are known.
- Contacts at the internet provider, content delivery network and any DDoS mitigation service are on the contact sheet.
- The service has redundancy, load balancing and a way to scale.
- Communications for customers are ready, with a way to post status away from the affected service.

Workflow

Work in this order. Record each step and its time in the incident log.

1. Confirm it is an attack: check for unavailability, network congestion, unusual traffic patterns, server crashes, high resource use and trouble reaching other services such as DNS.
2. Classify the technique: volumetric, protocol or application. The response differs by type.
3. Call the upstream provider or mitigation service and ask for filtering.
4. Apply filtering at the edge: rate limits, blocks on known malicious sources, and a challenge for web requests where suitable.
5. Keep customers informed through a channel that does not depend on the affected service.
6. After the attack: assess the impact, restore services, do a post-incident analysis, fix what was found and update the plan.

Decision points

Stop at each of these and record the decision, the decider and the time.

Decision	Who decides	Information needed
Switch to a mitigation service or failover?	Technical lead, executive sponsor	Attack type, cost, time to switch
Is the attack covering something else?	Incident lead	Other alerts, access attempts during the attack
What do we tell customers?	Communications lead	Impact, expected recovery time

Notices to check

Open section 10 of the plan and confirm whether any of these start a notice clock.

- A DDoS attack alone is an availability incident; check whether personal data was affected before treating it as a breach.
- Check contract service levels and customer notice terms.

Exit criteria and follow-up

Close the playbook only when all of these are true.

- Service restored to normal levels.
- Traffic patterns back to baseline for [period].
- The plan is updated with what was learned.