Denial-of-service attack (DDoS)

Version 1.0 · Reviewed Oct 11, 2026 · TLP:CLEAR · For: Infrastructure, network and online services leads.

What to do when a site or service stops responding because it is being flooded with traffic. The goal is to restore the service with your provider's help and verify that the attack is not hiding another intrusion.

Signs it is happening

- A site or application that is slow or unreachable for all users.
- A sudden increase in traffic from many addresses or from a single country.
- Bandwidth, CPU or server connections at their limit.
- An extortion message threatening an attack or claiming responsibility for one.

How serious it is

Critical	An essential public-facing service down for more than an hour, or an attack with extortion.
High	Service degraded for most users.
Medium	Attack absorbed by the protection, with minor impact.

First hour

- [ ] **1.** Confirm that it is an attack and not an internal failure or a legitimate spike in visits.
- [ ] **2.** Call your internet or hosting provider and open an emergency case.
- [ ] **3.** Turn on the protection mode of your CDN or WAF if you have one.
- [ ] **4.** Capture a sample of the traffic and save the logs before they rotate.
- [ ] **5.** Post a status notice through an alternate channel (social media, status page).
- [ ] **6.** Do not reply or pay if you receive an extortion message.

Preparation (before the incident)

- Put public services behind a CDN with anti-DDoS protection.
- Keep your provider's emergency contact and the mitigation procedure at hand.
- Know your normal traffic so you can recognize what is abnormal.
- Hide the origin IP address of your servers.

Detection and Analysis

- Identify the type: volumetric, protocol or application layer.
- Determine the exact target: IP address, port, URL or DNS service.
- Look for patterns: source countries, user agent, requested paths.
- Check whether there are intrusion attempts on other systems at the same time.

Containment

- Ask the provider for filtering on its network or diversion to a scrubbing center.
- Apply rate limits and country blocks if your audience is local.
- Turn on browser challenges on the paths under attack.
- Temporarily disable the most expensive features (searches, reports).

Eradication

- Change the origin IP address if it was exposed and restrict access to the CDN only.
- Close ports and services that should not be published.
- Fix any of your own services that could be used to amplify attacks.

Recovery

- Lift the restrictions in stages while you monitor the traffic.
- Keep the heightened protection in place for at least 72 hours: attacks tend to recur.
- Announce the restoration through the same channels as the initial notice.

Lessons Learned

- Document the duration, peak volume and impact on the service.
- Assess whether the contracted mitigation capacity was sufficient.
- Test the procedure with the provider at least once a year.

Evidence to preserve

- A traffic capture (PCAP) or flow logs from during the attack.
- Web server, firewall and CDN logs.
- Bandwidth and availability graphs.
- Extortion messages, with headers if they arrived by email.

What not to do

- Paying an extortion demand: it guarantees nothing and marks you as a target.
- Restarting servers over and over without having filtered the traffic.
- Blocking addresses by hand, one by one, in a distributed attack.
- Assuming it is only a DDoS: it may be a distraction.

Who to notify

- Your internet, hosting or CDN provider.
- Users and customers, with a clear status notice.
- Management, with the impact and the estimated time.
- The Public Ministry (Ministerio Público), if there was extortion.
- cert.gt, to correlate with attacks on other organizations.

When to close the incident

- The service has operated normally for 72 hours without extraordinary restrictions.
- The origin address is no longer directly reachable from the internet.
- A parallel intrusion has been ruled out.
- The mitigation contract or plan has been reviewed.

cert.gt is a private, community-driven initiative of Devel Group.

cert.gt · devel.group · Report an incident at cert.gt/en/reportar or email incidentes@cert.gt

General good-practice guidance; it does not replace legal or specialized technical advice for your case. This is not a document from a government entity. You may copy and adapt it with attribution (CC BY 4.0).