GAJWAF · INCIDENT PLAYBOOK

DDoS / Layer-7 flood

Keep the site and its backend alive under a request flood

Prove it's a browser. Cap every client.

A volumetric or request flood is overwhelming a site or its backend. GAJWAF defends the **application layer (L7)** — floods of HTTP requests, slow clients, bot swarms. It is **not** a network-layer scrubbing service. This playbook starts by drawing that line, then sheds the flood at L7 and escalates what it can't.

Seconds
For under-attack mode to bite

7 steps
Triage → contain → escalate → recover

1 record
For your incident log

GajShield Infotech Private Limited
Mumbai, India

Version 1.0 · October 2026
For GAJWAF analysts, administrators & network teams

LEGAL NOTICE

© 2026 GajShield Infotech Private Limited All rights reserved. This document is provided for the use of GAJWAF customers and partners. No part of it may be reproduced, distributed or transmitted in any form or by any means without the prior written permission of GajShield Infotech Private Limited

The information in this document is provided "as is", without warranty of any kind, express or implied, and is subject to change without notice. Features, menu labels and default values may differ between GAJWAF releases. While every effort has been made to ensure its accuracy, GajShield Infotech Private Limited accepts no liability for any loss, damage or service disruption arising from the use of, or reliance on, this document. This playbook is general operational guidance. It does not replace your organisation's own incident-response or change-control procedures, and GAJWAF is not a substitute for network-layer (L3/L4) DDoS protection.

GAJWAF and GajShield are trademarks of GajShield Infotech Private Limited Amazon Web Services, AWS and AWS Shield are trademarks of Amazon.com, Inc. or its affiliates. Microsoft and Azure are trademarks of the Microsoft group of companies. All other product and company names mentioned in this document are trademarks of their respective owners; they are used for identification purposes only, and their mention does not imply endorsement.

AT A GLANCE

Know the boundary

GOLDEN RULE

At L7, make every client **prove it's a real browser** and **cap how much any one client can ask for**. Under-attack mode plus rate limits and bans handle most floods.

A packet flood that saturates the link needs your cloud / network provider's DDoS protection — not the WAF.

L7 · GAJWAF handles it

Application layer — this playbook

- Floods of HTTP requests
- Slow clients (slowloris)
- Bot swarms hitting real URLs

L3 / L4 · Escalate it

Network layer — cloud / network team

- Link saturated, packets dropped
- UDP / SYN floods
- AWS Shield · Azure DDoS Protection · scrubber

TRIAGE	CONTAIN AT L7				ESCALATE	RECOVER
1 Classify the flood	**2** Under-attack mode	**3** Rate limits & auto-bans	**4** Cut the source	**5** Protect the backend	**6** Escalate L3/L4	**7** After it subsides

✕ DON'T

- **Don't** expect the WAF to absorb an L3/L4 volumetric DDoS — escalate instead of waiting.
- **Don't** set per-IP rate limits so low that real users behind shared NAT, corporate proxies or privacy relays get caught.
- **Don't** switch the site **Off** — that forwards the entire flood straight to the backend.
- **Don't** forget multi-node: bans and clearances only carry across nodes that share `cluster.secret`.

WHO **Analyst** for the live response; **admin** for standing rate-limit config; **network / cloud team** if it's volumetric.

CONTENTS

1 Classify the flood 3
2 Turn on under-attack mode 3
3 Tighten rate limits and auto-bans 4
4 Cut the source if it's concentrated 4
5 Protect the backend 5
6 Escalate to the network layer 5
7 After it subsides 6
✓ Back to normal & incident record 7

© 2026 GajShield Infotech Private Limited All rights reserved.

STEP 1 OF 7

1 Classify the flood

PHASE TRIAGE WHO Analyst TIME First — this decides everything

What you see	Layer	Who handles it
Huge HTTP request rate, bot-like clients, hitting real URLs or one endpoint	**L7**	**GAJWAF** — this playbook, Steps 2–5.
Slow / incomplete requests holding connections open	**L7** (slowloris)	**GAJWAF** connection / time limits.
Link saturated, packets dropped before reaching the WAF, UDP / SYN flood	**L3 / L4**	**Cloud / network DDoS protection** (AWS Shield, Azure DDoS Protection, upstream scrubber) — go to **Step 6**.

Check **Overview** and the server's own load:

If…	Then
Requests **are reaching the WAF** and being logged	It's **L7** — you can act here. Continue to Step 2.
The box or link is **saturated**, and traffic **isn't arriving as HTTP**	**Escalate to the network layer immediately** (Step 6) — the WAF can't fix what never reaches it.

✓ MOVE ON WHEN

You know whether this is an **L7** flood (act here) or an **L3/L4** flood (escalate).

STEP 2 OF 7

2 Turn on under-attack mode

PHASE CONTAIN WHO Analyst TIME Seconds — sheds most L7 floods

The primary L7 defence. On the affected site, click **"Under attack…"** and pick a duration. Every visitor must pass a **browser check** — which defeats the vast majority of flood bots, because they can't run it.

Client	During under-attack mode
Legitimate browsers	Pass once and are cleared for the session.
API-credentialed / auth-gateway clients	**Not challenged** — apps and integrations keep working.
Other non-browser clients	Your choice, under **Bot check → "Clients that cannot run the check"** (`challenge.non_browser`): **block** for a hard lockdown, or **allow** to keep them working while browsers are gated.

© 2026 GajShield Infotech Private Limited All rights reserved.

> **TIP**
> This alone sheds most L7 floods within seconds.

> **✓ MOVE ON WHEN**
> Request volume reaching the backend drops, and real browsers are getting through.

STEP 3 OF 7

3 Tighten rate limits and auto-bans

PHASE CONTAIN WHO Analyst · Admin for standing config

WHERE **Edit configuration → Rate limits & bans**

- **Tighten the per-IP request rate** so any single client is capped.
- **Lower the auto-ban threshold** so abusive clients are banned automatically — and stay out.
- **Ban known abusers by hand:** Bans page → **"+ Ban an IP"**, or review the auto-bans already accumulating.

> **NOTE**
> For a flood from **many IPs** (a botnet), under-attack mode does more than per-IP limits — **combine both**.

> **IMPORTANT**
> Don't set per-IP limits so low that real users get caught — especially those behind **shared NAT, corporate proxies or privacy relays**. For broad floods, prefer the browser check.

> **✓ MOVE ON WHEN**
> Single clients are capped, and repeat abusers are being auto-banned.

STEP 4 OF 7

4 Cut the source if it's concentrated

PHASE CONTAIN WHO Analyst · Admin

If the flood…	Do this	Where
Comes from **countries** or **hosting / cloud networks** you don't serve	Block them, or score them heavily. Floods often originate from cloud/hosting networks — **high yield, low collateral**.	**Geo & reputation** tab
Is pounding **one expensive URL**	Add a **Custom rule** (block, or a stricter rate) **scoped to that path** — the backend is protected while the rest of the site stays open.	**Custom rules** tab

© 2026 GajShield Infotech Private Limited All rights reserved.

✓ MOVE ON WHEN

Concentrated sources and hot endpoints are covered by a targeted control.

STEP 5 OF 7

5 Protect the backend

PHASE CONTAIN WHO Analyst TIME Throughout

The point of Steps 2–4 is to **keep the origin alive**. Watch it:

Signal	What it means	What to do
`upstream-error` events, **rising latency**	The backend is starting to buckle.	Make sure under-attack mode and rate limits are on — they cut the load the origin sees.
Backend **already down**	The WAF serves errors on its behalf.	Keep shedding the flood — that is what lets the backend come back.

✓ MOVE ON WHEN

Backend errors have stopped and latency is recovering.

STEP 6 OF 7

6 Escalate to the network layer

PHASE ESCALATE WHO Network / cloud team TIME Immediately, if volumetric

When to escalate: the link is saturated, the WAF or its host is unreachable, or traffic isn't arriving as HTTP. This is beyond L7.

Action	Detail
Turn on / lean on your cloud provider's DDoS protection	**AWS Shield** · **Azure DDoS Protection Standard** — or an upstream scrubbing / CDN service.
Confirm exposure is minimal	On a cloud deployment, the edge Security Group / NSG should already restrict exposure to **80/443** (and the console port to your management IP). Confirm nothing else is open.

IMPORTANT

Don't wait for the WAF to absorb an L3/L4 flood — it can't. Escalate as soon as you've classified it.

© 2026 GajShield Infotech Private Limited All rights reserved.

✓ MOVE ON WHEN

The network-layer protection is engaged, and HTTP traffic is reaching the WAF again.

STEP 7 OF 7

7 After it subsides

PHASE RECOVER WHO Analyst + admin

Measure	Keep or remove?
Under-attack mode	Let it expire — or end it once rates normalise.
Rate limits, geo / network blocks that proved useful	**Keep** as standing config.
Bans	Decide which to keep.

TIP

If floods recur: consider fronting the WAF with a CDN / scrubber permanently, and make under-attack thresholds (Bot check → **"Switch on automatically at"**) part of the site's baseline.

✓ MOVE ON WHEN

Temporary measures have a clear end, durable ones are in the standing config, and the incident is recorded.

© 2026 GajShield Infotech Private Limited All rights reserved.

CLOSE THE INCIDENT

✓ Back to normal & incident record

☐	**Request rate**	Back to baseline in **Overview**; `upstream-error` events gone.
☐	**Backend**	Latency and health are normal.
☐	**Real users**	Getting through — not stuck at the challenge.
☐	**Temporary measures**	Either expired or deliberately kept.

INCIDENT RECORD

Site(s) affected	
Started / detected at	
Layer	☐ L7 (HTTP flood) ☐ L7 (slowloris) ☐ L3 / L4 (volumetric)
Peak request rate / sources	
Incident ID(s)	
Measures taken	☐ Under-attack ☐ Rate limits ☐ Bans ☐ Geo ☐ Custom rule ☐ Escalated
Kept in standing config	
Ended at	
Handled by	

Related documents

Document	Use it for
Site under active attack (playbook)	Technique-based attacks rather than volume.
GAJWAF Features & Configuration Guide	Bot check & under-attack mode (ch. 7), Rate limits & bans (ch. 8), Geo & reputation (ch. 5), Custom rules (ch. 11).
GAJWAF Troubleshooting & Support Manual	Upstream errors (chapter A) and performance (chapter H).

© 2026 GajShield Infotech Private Limited All rights reserved.