GAJWAF · OPERATIONS PLAYBOOK

Hardening the **deployment**

No way around the WAF. No way into the console.

Two things must be true. Everything else is tuning.

A WAF only helps if traffic **can't go around it** and the console **can't be reached by attackers**. This is the checklist that closes both gaps — and produces a signed record you can hand to an auditor.

2 gaps
Bypass · management access

5 steps
Edge → origin → CDN → IP → console

7 checks
Pass / fail evidence record

GajShield Infotech Private Limited
Mumbai, India

Version 1.0 · October 2026
For GAJWAF 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

What a hardened deployment looks like

GOLDEN RULE

Two things must be true: the backend accepts traffic **only from the WAF**, and the management surfaces (console, SSH) are reachable **only from your admin network**.

Everything else is tuning.



✕ DON'T

- **Don't** leave the console or SSH open to the Internet.
- **Don't** leave the origin reachable from anywhere but the WAF.
- **Don't** trust `X-Forwarded-For` from an untrusted hop — set the trusted-proxy list correctly, or the client IP can be spoofed.

WHO **Admin** + whoever controls the **cloud network / firewall**.

CONTENTS

1 Lock the edge 3
2 Stop WAF bypass 3
3 Lock GAJWAF to your CDN 4
4 Make the real client IP trustworthy 4
5 Harden the console 5
✓ Hardening checklist 6

© 2026 GajShield Infotech Private Limited All rights reserved.

STEP 1 OF 5

1 Lock the edge

AREA NETWORK WHO Network / cloud team

WHERE The firewall in front of GAJWAF — **AWS Security Group** or **Azure Network Security Group (NSG)**

Port	Purpose	Allow from
80 / 443	Client web traffic	**The Internet** (or your CDN — see Step 3)
9443	GAJWAF management console	**Your management network (CIDR) only**
22	SSH	**Your management network only** — or keep it **closed** if you don't use it
Everything else	—	**Deny**

NOTE

The AWS and Azure Marketplace templates already apply most of this. Use this playbook to **verify** them — and as the build checklist for other deployments.

✓ MOVE ON WHEN

Only 80/443 are open to the Internet; 9443 and 22 are reachable from your management network only.

STEP 2 OF 5

2 Stop WAF bypass

AREA NETWORK WHO Network / cloud team

Put a firewall or security group on the **backend** so the origin accepts inbound traffic **only from the WAF** — its subnet or address.

IMPORTANT

Otherwise an attacker who learns the origin IP simply **skips the WAF** — and none of its protection applies.

✓ MOVE ON WHEN

The backend refuses any connection that doesn't come from GAJWAF.

© 2026 GajShield Infotech Private Limited All rights reserved.

STEP 3 OF 5 · IF APPLICABLE

3 Lock GAJWAF to your CDN

AREA NETWORK WHO Network / cloud team

Only if a CDN or Azure Front Door sits in front of GAJWAF.

Do this	Example
Restrict GAJWAF to accept traffic only from the CDN's address ranges.	Azure service tag `AzureFrontDoor.Backend` in the NSG.
Verify the CDN's instance header, so nobody can reach GAJWAF directly by spoofing the CDN.	Azure Front Door's `X-Azure-FDID` header, matched to your Front Door instance.

✓ MOVE ON WHEN

GAJWAF accepts web traffic only from your CDN — and only from your instance of it.

STEP 4 OF 5

4 Make the real client IP trustworthy

AREA TRUST WHO Admin + application team

Where	Do this	Why
Backend web server	Read the client IP from `X-Forwarded-For`, which GAJWAF sets — e.g. Apache `mod_remoteip` or the equivalent for your server.	Your application's logs show **real visitors**, not the WAF.
GAJWAF — Settings → Network trust & lists → "Trusted proxies"	List **every front proxy or CDN** in front of GAJWAF.	GAJWAF uses the true client IP for **geo, rate limits and bans** — and a client **can't spoof** it.

IMPORTANT

Never trust `X-Forwarded-For` from an untrusted hop. If the trusted-proxy list is wrong, the client IP can be **spoofed** — or every client looks like your CDN.

✓ MOVE ON WHEN

Application logs show real client IPs, and only your own proxies / CDN are trusted.

© 2026 GajShield Infotech Private Limited All rights reserved.

STEP 5 OF 5

5 Harden the console

AREA CONSOLE WHO Admin

WHERE **Settings → Management console** and **Settings → Console users**

1. Turn on **require login** and **two-factor authentication** for the console.
2. Create a **named admin user** for each operator (Settings → Console users), and stop relying on the bootstrap token for daily use.
3. **Rotate the first-boot bootstrap token** once real users exist.
4. Keep GAJWAF **up to date** — **Settings → Software update**.

✓ MOVE ON WHEN

The console requires login and 2FA, every admin has a named account, the bootstrap token is rotated, and the software is current.

© 2026 GajShield Infotech Private Limited All rights reserved.

VERIFY · KEEP AS COMPLIANCE EVIDENCE

✓ Hardening checklist

Test each item, record the result, and keep the completed page with your compliance records. (The *Compliance reporting* playbook pairs its report with this checklist.)

Step	Check	How to test	Pass	Fail
1	**Console & SSH closed** to the Internet; **80/443 open**	From a network **outside** your management range, open `https://<waf-ip>:9443/` in a browser — it must fail. Port 22 must not connect. The website must load.	☐	☐
2	**No WAF bypass**	Request the **origin IP directly**, from anywhere but GAJWAF — it must be refused.	☐	☐
3	**CDN-only** (if applicable)	A request to GAJWAF that doesn't come through your CDN — or carries the wrong instance header — must be refused.	☐	☐
4	**Real client IPs**	The application's own logs show **visitors' IPs**, not GAJWAF's.	☐	☐
5	**Console login + 2FA**	Signing in to the console asks for a password **and** a second factor.	☐	☐
5	**Bootstrap token rotated**	The first-boot token no longer works.	☐	☐
5	**Software current**	Settings → Software update shows no pending update.	☐	☐

Deployment / site(s)	
Cloud / platform	☐ AWS ☐ Azure ☐ Other: _____
Verified by	
Date	
Next review due	

Related documents

Document	Use it for
Compliance reporting (playbook)	Pairing this checklist with a GAJWAF report for an auditor.
Zero-downtime cutover (playbook)	Moving traffic onto GAJWAF without an outage.
GAJWAF Troubleshooting & Support Manual	Real client IP problems (chapter A).
GAJWAF Quick Setup Guide — AWS & Azure	Security group / NSG and console sign-in on first launch.

© 2026 GajShield Infotech Private Limited All rights reserved.