CDN and WAF configuration checklist for overseas traffic

An operations check kit that confirms cache correctness, legitimate requests and change recovery

A practical IXC resource for adoption decisions and delivery

Published 2026.09 · English edition · PDF + Excel worksheets

Using this resource

Finds refresh errors, blocked legitimate requests and origin exposure in a CDN and WAF configuration that is already in production.

CDN and WAF operators, overseas service owners and security review leads

Contents

01 Confirm the path real requests take 3

02 Check the cache and WAF with different questions 4

03 Configuration check and fix record 5

04 Continue observation and recovery after the change 6

How to complete and reuse it

Read the criteria in this PDF, then fill the blank fields with your actual conditions and anything still unconfirmed. The Excel file for the same practice area has a worksheet for each resource. Keep the worked examples separate from real customer cases and confirmed quotes.

With attribution, you may quote and adapt this material for internal review and your own work. The latest files are at www.ixc.co.kr/en/assets.

Confirm the path real requests take

Start by aligning the request path and the protection scope for each domain. Even when a setting exists in the management console, its effect cannot be confirmed unless real traffic passes through it.

List the public domains and API hosts, and link each one to its DNS, certificate, CDN configuration, WAF policy and origin. Distinguish production environments, test environments and bypass domains. Compare real requests with the policies applied to them in the access logs, then look for hosts that were left out. When restricting the direct origin path, also check the paths used by health checks and approved integrations.

Check item	Question	Evidence
DNS and hosts	Are all the domains in use included?	DNS responses and host list
TLS certificates	Are the names, expiry and renewal owner correct?	Certificate check and renewal path
Applied settings	Which version applies to real requests?	Request logs and configuration version
Origin access	Are bypass paths kept distinct from allowed requests?	Access policy and integration tests

> **Baseline before a change**
>
> Save the response headers of representative URLs, the results of normal business flows, origin request volume and recent block history. Tracing the cause and recovering are only possible if the same requests can be rerun after the change.

Check the cache and WAF with different questions

For the cache, confirm that it reuses correct responses; for the WAF, confirm that it applies the block policy while letting legitimate requests through. Do not judge both by a single metric.

Path	Cache question	WAF question
Static files	Are versioning, retention and invalidation right?	Are requests for allowed files blocked?
Sign-in and member pages	Does user data remain in a shared cache?	Do legitimate authentication requests get through?
Search and upload	Are responses that differ per request kept apart?	Are inputs of normal length and format blocked?
Payment flows and webhooks	Is the policy right for sensitive and state-changing responses?	Do legitimate server-to-server calls get through?

Evaluation in Akamai App & API Protector is a mode for previewing how new hosts would be handled under the current security configuration. For actual enforcement, check the contracted features and the policies in the management console. Do not judge security to have improved from a rise in block volume alone; investigate the rise together with failures in normal business flows. Rather than a broad exception for a whole path, narrow down the conditions of the false-positive requests and the scope of what needs to be allowed.

> **Worked example**
>
> A legitimate request to register a product, with special characters in its description, was blocked. Reproduce the request path, the rule and the input conditions, then review how those conditions are handled. Before allowing the entire admin path, test other legitimate and abnormal requests as well.

Configuration check and fix record

Record each verdict as OK, Issue or Unconfirmed. Unconfirmed is not a pass: assign the requests to check and an owner. After a fix, run the same test again.

CDN and WAF change verification sheet

Check question	Evidence and test request	Verdict and observation	Fix and owner
Are responses separated by user?	Same URL from different accounts		
Do content replacements take effect?	Replacement, invalidation and re-request		
Do normal purchases and uploads succeed?	Reproduced core business flows and block log		
Do the protected hosts match?	DNS, policy and access logs		
Can the previous settings be restored?	Configuration versions and restore test		

Check requests must not carry raw personal data or secret values; use the structure needed for reproduction and de-identified samples. Also decide who may view production logs and where they are stored. Check high-impact settings in an approved test environment first. If a change has to go to production, record the change window, the observation owner and the stop criteria together in the change record.

> **Pass criteria**
>
> Record OK only when functional tests pass and responses are correct, with the applied version and logs linked. If only speed or block volume has improved, leave the remaining items as Unconfirmed and continue the check.

Continue observation and recovery after the change

Cache and block settings need rechecking with releases, new features and changes in traffic. Recording why a change was made and which version to roll back to speeds up the response.

- Before cutover, preserve the baseline of normal business flows and the configuration version. Keep certificate and origin access changes as separate check items.
- After the change, observe regional responses and errors, origin requests, cache hits and blocked legitimate requests together.
- If a problem appears, compare the time the change was applied with the request evidence. Restore the approved previous settings, then recheck core business flows.
- Record a reason, owner and next review date for each exception rule. Review them so that temporary allowances do not stay on as permanent settings.

When a new API or upload method is released, send the request format to the security operator. When content file paths change, also review the cache rules and invalidation targets. Even when development, security and infrastructure sit with different vendors, omissions drop only when the owners who receive change notices and the approval path are linked in one record.

> **Scope to work on with IXC**
>
> IXC handles WAF rule design and false-positive adjustment, DDoS defence, certificates and access control. Together with CDN operations, we set the scope for checking request paths, caching and security policy.

Publication and use

We set what to check based on your domains and representative URLs, cases where legitimate requests were blocked, your current configuration and its change history.

IXC Corp.

CEO Nam Kichul | Business registration no. 109-86-56732
4F 408, Chuncheon ICT Venture Center
7 Huseok-ro 462beon-gil, Chuncheon-si, Gangwon-do, Republic of Korea
+82-33-242-0210 | info@ixc.co.kr

www.ixc.co.kr

www.ixc.co.kr/en/services/web-security

www.ixc.co.kr/en/assets/cdn-waf-checklist

References

Akamai: Learn about caching

https://techdocs.akamai.com/property-mgr/docs/know-caching

Akamai: App & API Protector

https://techdocs.akamai.com/cloud-security/docs/app-api-protector

IXC Web Security — WAF & DDoS

https://www.ixc.co.kr/en/services/web-security