
CDN·WAF 구성 점검표 · 해외 접속

캐시 정확성, 정상 요청, 변경 복구를 확인하는 운영 점검 키트

도입 판단과 실행을 위한 IXC 실무 자료

2026.09 발행 · 한국어판 · PDF + Excel 작성 서식

이 자료의 활용

이미 운영 중인 CDN·WAF 설정에서 갱신 오류와 정상 요청 차단, 원본 노출 문제를 찾습니다.

CDN·웹방화벽 운영자·해외 서비스 담당·보안 점검 책임자

목차

01	실제 요청이 거치는 경로를 확인합니다	3
02	캐시와 WAF는 다른 질문으로 점검합니다	4
03	설정 점검과 수정 기록표	5
04	변경 후 관측과 복구를 이어갑니다	6

작성과 활용

PDF의 기준을 읽고 빈 작성란에 실제 조건과 미확인 항목을 적습니다. 같은 부문의 Excel에는 자료별 작성 시트가 있습니다. 작성 예시는 실제 고객 사례나 확정 견적과 구분해 사용합니다.

출처를 밝히면 사내 검토와 업무 수행에 인용·수정하여 사용할 수 있습니다. 최신 파일은 www.ixc.co.kr/assets에서 확인할 수 있습니다.

실제 요청이 거치는 경로를 확인합니다

도메인별 요청 경로와 보호 범위를 먼저 맞춥니다. 관리 화면에 설정이 있어도 실제 트래픽이 그 설정을 지나지 않으면 효과를 확인할 수 없습니다.

공개 도메인과 API 호스트를 목록으로 만들고 DNS, 인증서, CDN 설정, WAF 정책, 원본을 연결합니다. 운영·시험 환경과 우회용 도메인을 구분합니다. 접근 기록에서 실제 요청과 적용 정책을 대조한 뒤 빠진 호스트를 찾습니다. 원본 직접 경로를 제한할 때는 상태 점검과 승인된 연동이 사용하는 경로도 확인합니다.

점검 항목	질문	증거
DNS·호스트	사용 중인 도메인이 모두 포함되니까?	DNS 응답·호스트 목록
TLS 인증서	이름·만료·갱신 담당이 맞습니까?	인증서 확인·갱신 경로
적용 설정	실제 요청에 어떤 버전이 적용되니까?	요청 로그·설정 버전
원본 접근	우회 경로와 허용 요청이 구분되니까?	접근 정책·연동 시험

변경 전 기준선

대표 URL의 응답 헤더, 정상 업무 결과, 원본 요청량과 최근 차단 이력을 저장합니다. 변경 뒤 같은 요청을 재실행할 수 있어야 원인 추적과 복구가 가능합니다.

캐시와 WAF는 다른 질문으로 점검합니다

캐시는 올바른 응답을 재사용하는지, WAF는 정상 요청을 통과시키면서 차단 정책을 적용하는지 확인합니다. 한 지표로 둘을 판단하지 않습니다.

경로	캐시 질문	WAF 질문
정적 파일	버전·보관·무효화가 맞습니까?	허용 파일 요청이 막힙니까?
로그인·회원	사용자 정보가 공유 캐시에 남습니까?	정상 인증 요청이 통과합니까?
검색·업로드	요청별 다른 응답을 구분합니까?	정상 길이·형식이 차단됩니까?
결제·웹훅	민감·변경 응답의 정책이 맞습니까?	서버 간 정상 호출이 통과합니까?

Akamai App & API Protector의 Evaluation은 새 호스트가 현재 보안 설정에서 어떻게 처리될지 미리 확인하는 모드입니다. 실제 적용에서는 계약된 기능과 관리 화면의 정책을 확인합니다. 차단량 증가만으로 보안 개선을 판정하지 않고 정상 업무 실패와 함께 조사합니다. 경로 전체를 넓게 예외 처리하기보다 오탐 요청의 조건과 필요한 허용 범위를 좁힙니다.

작성 예시

상품 설명에 특수문자가 들어간 정상 등록 요청이 차단됐습니다. 요청 경로와 규칙, 입력 조건을 재현한 뒤 해당 조건의 처리 방식을 검토합니다. 관리자 전체 경로를 허용하기 전에 다른 정상·비정상 요청을 함께 시험합니다.

설정 점검과 수정 기록표

판정은 정상·문제·미확인으로 기록합니다. 미확인은 통과가 아니며 확인할 요청과 담당을 배정합니다. 수정 후에는 같은 시험을 다시 수행합니다.

CDN·WAF 변경 검증표

점검 질문	증거·시험 요청	판정·관측값	수정·담당
사용자별 응답이 구분됩니까?	서로 다른 계정의 동일 URL		
콘텐츠 교체가 반영됩니까?	교체·무효화·재조회		
정상 구매·업로드가 성공합니까?	핵심 업무 재현·차단 로그		
보호 대상 호스트가 일치합니까?	DNS·정책·접근 기록		
이전 설정으로 복구됩니까?	설정 버전·복구 시험		

점검 요청에는 개인 정보와 비밀 값을 그대로 남기지 않고 재현에 필요한 구조와 비식별 표본을 사용합니다. 운영 로그를 열람할 권한과 보관 위치도 정합니다. 영향이 큰 설정은 승인된 시험 환경에서 먼저 확인합니다. 운영 적용이 필요하면 작업 창, 관측 담당, 중단 기준을 변경 기록에 함께 적습니다.

통과 기준

기능 시험과 응답 정확성이 맞고 적용 버전·로그가 연결돼야 정상으로 판정합니다. 속도나 차단량 하나만 좋아진 경우에는 나머지 항목을 미확인으로 남기고 점검을 이어갑니다.

변경 후 관측과 복구를 이어갑니다

캐시·차단 설정은 배포, 신규 기능, 트래픽 변화에 맞춰 다시 점검해야 합니다. 변경한 이유와 되돌릴 버전을 남기면 대응이 빨라집니다.

- 전환 전 정상 업무 기준선과 설정 버전을 보존합니다. 인증서와 원본 접근 변경은 별도 확인 항목으로 둡니다.
- 변경 후 지역별 응답과 오류, 원본 요청, 캐시 적중과 정상 요청 차단을 함께 관측합니다.
- 문제가 생기면 적용 시각과 요청 증거를 대조합니다. 승인된 이전 설정으로 복구한 뒤 핵심 업무를 재확인합니다.
- 예외 규칙마다 사유·담당·재검토일을 기록합니다. 임시 허용이 영구 설정으로 남지 않도록 리뷰합니다.

새로운 API나 업로드 방식이 배포될 때는 보안 운영자에게 요청 형태를 전달합니다. 콘텐츠 파일 경로가 바뀌면 캐시 규칙과 무효화 대상도 검토합니다. 개발·보안·인프라가 다른 업체여도 변경 알림을 받는 담당과 승인 경로를 하나의 기록에 연결해야 누락을 줄일 수 있습니다.

IXC와 진행할 범위

IXC는 웹방화벽 규칙 설계와 오탐 조정, DDoS 방어, 인증서와 접근 통제를 다룹니다. CDN 운영과 함께 요청 경로·캐시·보안 정책을 점검할 범위를 정합니다.



발행·이용 안내

도메인과 대표 URL, 정상 요청 차단 사례, 현재 설정과 변경 이력을 기준으로 점검 대상을 정합니다.

아이엑스씨(주) · IXC

대표 남기철 | 사업자등록번호 109-86-56732
강원특별자치도 춘천시 후석로462번길 7
춘천ICT벤처센터 4층 408호
033-242-0210 | info@ixc.co.kr

www.ixc.co.kr

www.ixc.co.kr/services/web-security
www.ixc.co.kr/assets/cdn-waf-checklist

참고 자료

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 웹방화벽·DDoS 방어

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