ICS 33.040.40
CCS M16

Social Organization Standard

T/GBA 016—2024

Security and compliance technical requirements for Content Delivery Network（CDN）

内容分发网络（CDN）安全及合规技术要求

(English Translation)

Issue date: 2024-03-14 Implementation date: 2024-04-14

Issued by Guangdong-Hong Kong-Macao Greater Bay Area Standards Innovation Alliance

Contents

Foreword

This stabdard is drafted in accordance with the rules set forth in GB/T 1.1-2020 *Directives for Standardization -- Part 1: Rules for the Structure and Drafting of Standardizing* Documents.

This standard is proposed by the Industrial Internet Committee of the Greater Bay Area Standard Innovation Alliance.

The Standard is under centralized management by Guangdong-Hong Kong-Macao Greater Bay Area Standard Innovation Alliance.

This standard is authorized to be used by the partners and all member units of the Greater Bay Area Standard Innovation Alliance. Alliance partners are required to adopt and transform this Standard into their own group standards, and publicly disclose the basic information of the standard on the national group standard information platform.

Attention is drawn to the possibility that some of the elements of this standard may be the subject of patent rights. The issuing body of this document shall not be held responsible for identifying any or all such patent rights.

This is the first release.

Security and compliance technical requirements for Content delivery Network (CDN)

1 Scope

This document specifies the security and compliance technical requirements for Content Delivery Network (CDN) at different stages of content acceleration.

This document is intended to provide guidance for the design and implementation of content delivery services for network service providers.

2 Normative References

The contents contained in the following documents shall constitute essential clauses of the document through normative referencing.For the dated references,only the version corresponding to the date is applicable to the document;For the references undated,their latest versions (including all amendments) are applicable to the documents.

YD/T 4380-2023 *Technology Requirement for Content Delivery Network-Service Overview*

3 Terms and Definitions

The following terms and definitions are applicable to the document.

3.1 Content Delivery Network

The ability to dynamically redirect user requests to the nearest service node based on real-time information such as network traffic,connectivity and load status of each node, as well as the distance and response time to the user.The purpose is to enable users to access the desired content from the closest location,alleviate internet congestion,and provide faster response times for accessing websites.

3.2 Content Origin-Pull

When a user accesses certain content,but the CDN node does not have the content cached or the cached content has expired,the CDN will retrieve the content from the origin website and cache it on the CDN node for user access.

4 Abbreviation

The following abbreviations are applicable to the document.

Acknowledge Character (ACK)

Robot (BOT)

Challenge Collapsar (CC)

Content Delivery Network (CDN)

Cross Site Request Forgery (CSRF)

Distributed Denial-of-Service (DDoS)

Domain Name System (DNS)

Domain Validated (DV)

Extended Validated (EV)

Finish (FIN)

HTTP Strict Transport Security (HSTS)

Hypertext Transfer Protocol Secure (HTTPS)

Internet Control Message Protocol (ICMP)

Network Time Protocol (NTP)

Online Certificate Status Protocol (OCSP)

Organization Validated (OV)

Open Web Application Security Project (OWASP)

Quick UDP Internet Connections (QUIC)

Reset (RST)

Secure Sockets Layer (SSL)

Simple Service Discovery Protocol (SSDP)

Synchronization (SYN)

Transmission Control Protocol (TCP)

User Datagram Protocol (UDP)

Web Application Firewall (WAF)

Cross Site Scripting (XSS)

5 Overview

Content Delivery Network (CDN) is a distributed network that operates on the application layer, built upon existing infrastructure networks. It relies on the caching ability of nodes distributed at the network edge to reduce access pressure on the origin server, enabling end-users to access content nearby, avoiding network congestion and accelerating content access speed. As shown in Figure 1, CDN are located between the origin servers and the end-user access side, mainly consisting of load balancing system, caching system, origin pull system, and distribution system.

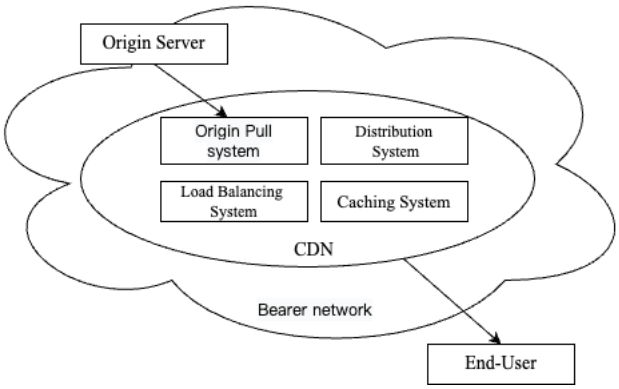

Figure 1: Content Delivery Network Diagram

CDN accelerates content delivery, and provides excellent user experience, but also requires security and compliance in the process. This document mainly provides technical requirements for security and compliance for content delivery network. Security and compliance for CDN include transmission security, access control, content tamper-proofing, content compliance, network security, and resource security, among others.

6 Content Transmission Security

6.1 HTTPS

CDN supports HTTPS, including:

The nodes of CDN should support clients accessing accelerated content via HTTPS.

a) CDN should support accessing the content from the origin server via HTTPS;

b) CDN should support enhanced capabilities for HTTPS, including force redirection, OCSP enable/disable, HSTS enable/disable.

6.2 QUIC

CDN should support accelerated websites being accessed via QUIC.

6.3 Certificate Management

CDN should meet the following requirements for certificate management security:

a) CDN should support security certificate management, including certificate uploading, publishing, updating and deleting;

b) CDN should support different types of certificates, including DV SSL certificates, OV SSL certificates, EV SSL certificates, etc;

c) CDN should support SSL certificates using the SM2/SM3 cryptographic algorithms to prevent sensitive information loss;

d) CDN should be able to support encrypted storage of certificates to prevent certificate leakage and support encryption storage using national cryptographic algorithms suites.

7 Access Control

7.1 Hotlink Protection

CDN supports Hotlink protection, including:

a) CDN should support the referer hotlink protection and support the management of Referer blocklist and allowlist configurations, including adding, modifying, and deleting the list. After a user's request reaches the CDN node, CDN can identify and determine the request's source identity based on the configured Referer blocklist and allowlist. If the referer field of a request matches the string configured in the allowlist, CDN node will return the requested information. However, If the referer field of a request matches the string configured in the blocklist, CDN node will not return the requested information and status code will be returned;

b) CDN should also support timestamp hotlink protection. When a client initiates a request, it needs to carry a signature to the server. The CDN node will perform server verification and only allow access after the verification passes. CDN should support the enabling and disenabling of this feature, as well as provide multiple signature algorithms for customers to choose from;

7.2 IP Blocklist/Allowlist

To effectively control the access sources of accelerated content, CDN should support IP blocklist/allowlist access control. By configuring an access control policy on IPs of user requests, CDN can effectively control the source of access, preventing hotlinking by malicious IPs, attacks, etc. Requirements are as follows:

a) CDN should support the management of IP blocklist/Allowlist access control policies, such as adding, modifying and deleting them. When a client's request reaches a CDN node, the node can effectively identify and judge the legality of the client’s IP based on the blocklist/allowlist;

b) When a client's request reaches a CDN node, the node can effectively identify and judge the legality of the client’s IP based on the blocklist/allowlist access control policy. If the client’s IP matches the allowlist access policy, the accessed node will return the requested resource, but if it matches the access policy in the blocklist, the accessed node will return status code directly;

c) CDN should support both IPv4 and IPv6 addresses.

7.3 IP Access Limit

CDN should support IP access limit by limiting the number of requests per second from a single IP address to a single node. Requirements are as follows:

a) CDN should support turning on and off the IP access limit function;

b) CDN should support setting and modifying the IP access frequency threshold;

c) When the IP access limit is enabled, CDN nodes can monitor and count the access of a single IP within a unit time. Status code will be returned for requests that exceed the QPS limit and CDN generates corresponding alarms;

d) CDN should support both IPv4 and IPv6 addresses.

7.4 UA Blocklist/Allowlist

CDN should support identifying and tracking the User-Agent HTTP header field, and according to this field, create rules to implement access control, improving the security of business resource access. Requirements are as follows:

a) CDN should support enabling and disabling the UA access control function;

b) CDN can set block and allowlist access control policies for UA and support adding, deleting, modifying, and querying policies;

c) When user requests arrive at the CDN node, CDN can recognize the UA field and determine whether to return the requested resource based on the block and allowlist policy. If the UA field hits the blocklist access policy, then it returns the status code directly. If it hits the allowlist access policy, it returns the requested resource.

8 Content Tamper-proofing

CDN supports content delivery to accelerate content access speed, which requires caching the origin content at the nodes. CDN should ensure that the content is not tampered with during the process of origin pulling, transmission between nodes, caching at the nodes, and pulling content from the nodes:

a) To support content origin integrity protection, CDN should provide verification mechanisms when retrieving content from the origin server, ensuring consistency of the content;

b) During a content transmission between nodes, CDN should provide a verification mechanism to maintain content consistency;

c) When content is stored on the nodes, CDN should provide a checking mechanism to periodically check the content consistency between the nodes and the source station content;
d) To ensure that content is not tampered with when accessed from the nodes, CDN should support a secure and reliable transmission protocol.

9 Content Compliance

9.1 Content Detection

9.1.1 Integration with Third-party Content Security Audit Systems

CDN should have the ability to integrate with third-party content security review systems to detect illegal or irregular content in text, images, and videos.

9.1.2 Abnormal Content Detection

CDN should meet the following requirements for abnormal content detection:

a) CDN should support abnormal content detection against illegal activities such as pornography, fraud and violence, by utilizing third-party recognition libraries;
b) CDN supports abnormal content archiving, recording business domain names, URLs, detection times and abnormal screenshots;
c) CDN should provide an open interface for abnormal data reporting to external parties, while recording the reporting status and time.

9.1.3 Custom Detection

CDN should support the customization of recognition libraries, allowing customers to define non-compliant content. The system can then identify related images, texts, and videos based on the content of the recognition libraries.

9.2 Abnormal Content Management

9.2.1 Website List Management

CDN should meet the following requirements for website list management:

a) CDN should have the ability to record and update a list of suspected illegal and non-compliant websites, which should at least include the domain name, IP, type of illegal and non-compliant activity, traffic, suspected discovery time, start and last access time, processing status and other information;
b) CDN should update the website list in real-time;
c) CDN should be able to support the long-term storage and query of the list of suspected illegal and non-compliant websites.

9.2.2 Access Log Management

CDN should support website monitoring by having the ability to save and query CDN access logs:

a) CDN should support access log retention, and the log information should include at least the access URL, source IP, source port, destination IP, destination port, and access time;
b) CDN should support customizing the access log retention period according to customer or regulatory requirements;
c) CDN should support log searching based on domain name and period, providing a search interface that regulatory authorities can use for querying logs;
d) CDN should support the access logs downloading.

9.2.3 Quick Cache Clearing

CDN should have the following capabilities for quick cache clearing:

a) CDN should support the quick clearing of caches for potentially illegitimate and illegal content across all nodes of the network;
b) CDN should have the ability to isolate illegal and non-compliant content,White suspected illegal and non-compliant content is detected.

9.3 Regulatory System Integration

CDN should be able to meet local regulatory requirements and could integrate with the information security management systems in Guangdong Province and Hong Kong/Macau regions.

10 Network Security

10.1 Security Protection

CDN should support DDoS protection,Web protection,Bot mitigation to ensure that CDN services are not affected by various network attacks and prevent service disruptions:

a) CDN should support DDoS protection,which includes protection service against network layer DDoS attacks by filtering UDP Flood, SYN Flood,TCP Flood,ICMP Flood,ACK Flood, FIN Flood,RST Flood,DNS/NTP/SSDP reflection attacks,and empty connections. Additionally,it should support application layer DDoS attack protection by filtering CC attacks and support HTTP custom feature filtering such as HOST filtering,User-agent filtering, and Referer filtering;
b) CDN should provide the WAF (Web Attach Firewall) to protect web applications from a variety of application layer attacks such as cross-site scripting (XSS),SQL injection,and cookie poisoning, among others;
c) CDN should support BOT mitigation,effectively defending against public types of BOTs such as search engines,speed testing tools,content aggregators,scanners,and web crawlers,and setting protection rules based on protocol features that include User-Agent categories,HTTP headers,and HTTP protocol features;
d) CDN should support configuration of protection strategies and provide protection statistical reports.

10.2 Security Alarm

CDN should support security monitoring and alarm,which can promptly detect the security status of CDN and take appropriate actions.Requirements are as follows:

a) CDN's security monitoring and alarm should support the definition of alarm rules, including alarm types,alarm conditions,and frequency settings;
b) CDN should support alarm notification,including SMS,voice,and telephone,etc.

10.3 Security Protection Level

In terms of security protection levels,CDN should meet the following requirements:

a) CDN should meet network security compliance requirement.The CDN system within Guangdong province should at least comply with the third-level certification of national network security level protection,and meet the corresponding requirements for security communication network,security area boundary,security computing environment,security management center,and security expert services;
b) CDN in Hong Kong and Macao should support at least level 2 or above CSA STAR security certification,and optional support for level 3 or above security protection

certification.

11 Resource Security

11.1 Resource Coverage

CDN should meet the following requirements for resource coverage:

a) CDN should have the capability to deploy enough notes all over the world. Within the Guangdong province, there should be at least one node in Guangzhou and Shenzhen to ensure that the local coverage rate of users visiting within Guangdong province is not less than 90%. There should be at least one node in Hong Kong and Macau region;
b) The nodes of CDN should meet the performance requirements of business acceleration, ensuring that content access speed can be increased by at least 30%, the success rate of access is greater than 99%, the average time to receive the first byte is less than 2 seconds, the image download rate (640K) is greater than 700KB/s, the download time for images (640K) is less than 2 seconds, the download speed for large files (8M) is greater than 1200KB/s, and the download time for large files (8M) is less than 8 seconds.

11.2 Resource Isolation

CDN should meet the following requirements for resource isolation:

a) CDN should support nodes isolation and allow the use of dedicated acceleration nodes to ensure that specified content is not extensively accelerated and cached to prevent leaks;
b) The CDN should support nodes insolation, including origin nodes, regional center nodes, and edge nodes;
c) The CDN should support isolation strategy configuration, enabling the specification of domains, acceleration nodes, and access control;
d) CDN should support isolated node monitoring and provide access logs.

11.3 Resource Compliance

CDN should meet the following requirements for resource compliance:

a) CDN should ensure the safety and reliability of hardware resource, and the procurement of node resources should come from IDC data centers and resource vendors with domestic or Hong Kong/Macau IDC operation licenses that comply with regulations;
b) IDC can ensure the availability of node operations, as well as have a complete monitoring and management system to ensure the physical security of resources and prevent illegal theft or tampering of cached content;
c) CDN should be able to detect gray node resource access, and must monitor the resource status of nodes, including operating system, CPU, memory, and bandwidth.

11.4 Resource Redundancy

CDN should meet the following requirements for resource redundancy:

a) CDN should support redundant deployment, including backup of scheduling system, operation system, and edge nodes. In Guangdong Province, Hong Kong, and Macao regions, dual system backup should be available. In case of failure, the switch should be made within a specified time;
b) CDN should support redundant deployment of core system links, redundant backup of multiple network access links, and redundant backup of communication network links between systems;
c) CDN should support system capacity redundancy setting, with at least 20% redundancy

capacity available to handle business requests during peak periods.

Bibliography

[1] GB/T 22239-2019 Information security technology-Baseline for Classified protection of cybersecurity.

[2] CSA 0001-2016 Cloud Computing Security Technology Requirement (CTSR).