ICS 33.040.40
CCS M16

团　　体　　标　　准

T/SZAS 79—2024

内容分发网络（CDN）安全及合规技术要求

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

2024-03-14 发布　　2024-04-14 实施

深圳市标准化协会　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由粤港澳大湾区标准创新联盟工业互联网委员会提出。

本文件由粤港澳大湾区标准创新联盟归口。

本文件授权粤港澳大湾区标准创新联盟组织伙伴和所有成员单位使用，联盟组织伙伴需等同采用转化为自身团体标准，并在全国团体标准信息平台上公开标准基本信息。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件起草单位：云宙时代科技有限公司、深圳市腾讯计算机系统有限公司、中国联合网络通信集团有限公司、深圳市标准化协会、澳门大学科技学院、云安全联盟大中华区、上海挪华威认证有限公司、ThoughtWorks。

本文件主要起草人：王妹、张鼎、栾亚建、王凌升、周志文、王永霞、黄超、吕华、但丹、黄承发、许木娣、韩放、蔡序娟、杨璐。

本文件为首次发布。

内容分发网络（CDN）安全及合规技术要求

1 范围

本文件规定了内容分发网络（CDN）在内容加速不同环节的安全及合规技术要求。

本文件适用于为提供内容分发服务的网络服务商提供设计和实施的指导。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

YD/T 4380-2023 内容分发网络技术要求 服务总览

3 术语和定义

下列术语和定义适用于本文件。

3.1

内容分发网络 Content Delivery Network

能够实时地根据网络流量和各节点的连接、负载状况以及到用户的距离和响应时间等综合信息将用户的请求重新导向离用户最近的服务节点上，其目的是使用户可就近取得所需内容，解决Internet网络拥挤的状况，提供用户访问网站的响应速度。

3.2

内容回源 Content Origin-Pull

当用户访问某个内容，但CDN节点上没有缓存该内容或者缓存的内容过期时，CDN会从源网站获取内容，并缓存在CDN节点上提供给用户访问。

4 缩略语

下列缩略语适用于本文件。

ACK：确认字符（Acknowledge Character）
BOT：机器人（Robot）
CC：挑战黑洞（Challenge Collapsar）
CDN：内容分发网络（Content Delivery Network）
CSRF：跨站请求伪造（Cross Site Request Forgery）
DDoS：分布式拒绝服务（Distributed Denial-of-Service）
DNS：域名系统（Domain Name System）
DV：域名校验（Domain Validated）
EV：扩展校验（Extended Validated）
FIN：终止（Finish）
HSTS：HTTP 严格传输安全性（HTTP Strict Transport Security）
HTTPS：超文本传输安全协议（Hypertext Transfer Protocol Secure）
ICMP：互联网控制消息协议（Internet Control Message Protocol）
NTP：网络时间协议（Network Time Protocol）
OCSP：在线证书状态协议（Online Certificate Status Protocol）

OV：组织校验（Organization Validated）
OWASP：开放式Web应用程序安全项目（Open Web Application Security Project）
QUIC：互联网快速链接（Quick UDP Internet Connections）
RST：复位（Reset）
SSDP：简单服务发现协议（Simple Service Discovery Protocol）
SSL：安全套接层协议（Secure Sockets Layer）
SYN：同步（Synchronization）
TCP：传输控制协议（Transmission Control Protocol）
UDP：数据报协议（User Datagram Protocol）
WAF：应用程序防火墙（Web Application Firewall）
XSS：跨站脚本（Cross Site Scripting）

5 概述

内容分发网络（CDN）是建设在现有基础网络之上的应用层分布式网络，依靠分布在网络边缘位置的节点的缓存能力来减少源站服务的访问压力，让最终用户可就近访问内容，避免网络拥塞，加速内容访问速度。如图1所示，CDN位于源服务站和最终访问用户之间，主要由负载均衡系统、缓存系统、回源系统、分发系统组成。

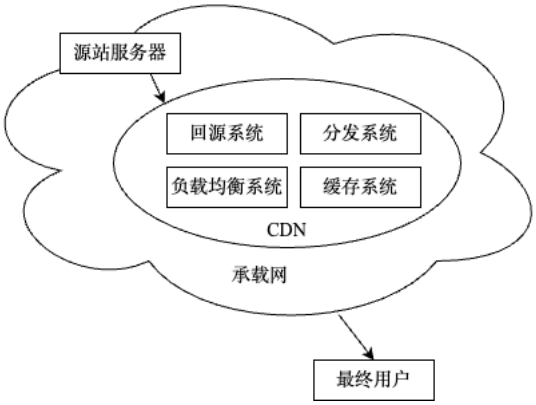

图 1:内容分发网络示意图

CDN 加速促进内容快速有效被访问，提供优良的用户体验，但同时也需要保证内容在加速过程的安全及合规。本文主要针对内容分发网络的安全及合规进行技术要求，CDN 的安全及合规包含传输安全、访问控制、内容防篡改、内容合规、网络安全、以及资源安全等。

6 传输安全

6.1 HTTPS 传输协议

CDN 应满足以下 HTTPS 传输协议安全要求：

a) CDN 应支持加速网站的 HTTPS 访问和回源，既要求 CDN 节点支持 HTTPS 访问，又要支持 CDN 能通过 HTTPS 协议访问源站拉取网站内容进行加速；
b) CDN 应支持 HTTPS 的加强能力，包含强制跳转、OCSP 启动/关闭、HSTS 启动/关闭。

6.2 QUIC 传输协议

CDN 应支持加速网站的 QUIC 访问，即 CDN 节点支持客户端通过 QUIC 访问。

6.3 证书管理

CDN 应满足以下证书管理安全要求：

a) CDN 支持安全传输协议，应具备证书管理能力，支持证书上传、发布、更新、删除等操作；
b) CDN 应支持不同类型证书，包含 DV SSL 证书、OV SSL 证书、EV SSL 证书等；
c) CDN 应支持通过 SM2/SM3 国密算法的 SSL 证书，以防止敏感信息丢失；
d) CDN 应支持证书加密存储以防证书泄漏，应支持国密算法套件加密存储。

7 访问控制

7.1 防盗链

CDN支持防盗链要求如下：

a) CDN 支持 Referer 防盗链，应能支持 Referer 黑白名单配置管理，包含新增、修改、删除功能。当用户访问到达 CDN 节点后，CDN 能根据配置的 Referer 黑白名单，对访问的身份进行识别判断，若符合白名单规则，则允许内容被访问；如果符合黑名单规则， CDN 节点拒绝返回该请求信息，直接返回状态码；
b) CDN 还应支持时间戳防盗链，客户端在发起请求时需要携带签名至服务端，CDN 节点进行服务端校验，校验通过后才继续放行访问。应支持该功能的开启及关闭，同时提供多种签名算法供用户选择。

7.2 IP 黑白名单

为了有效控制加速内容的访问来源，CDN应支持IP黑白名单访问控制，通过对用户请求端 IP 配置访问控制策略，有效限制访问来源，阻拦恶意 IP 盗刷、攻击等问题.要求如下：

a) 应支持 IP 黑白名单的访问控制策略管理，包含控制策略的新增、修改、删除功能；
b) 当用户访问到达 CDN 节点，CDN 节点能根据黑白名单访问控制策略有效识别判断访问 IP 的合法性，若访问来源 IP 符合白名单访问策略，则返回访问资源；若访问来源 IP 符合黑名单中的访问策略，则直接返回状态码；
c) 应支持 IPv4 和 IPv6 地址。

7.3 IP 访问限频

CDN 应支持 IP 访问限频，对单 IP 单节点在每一秒钟的访问次数进行限制，具体要求如下：

a) CDN 应支持 IP 访问限频功能的开启及关闭；
b) CDN 应支持 IP 访问频率的阀值进行设置及修改；
c) 当 IP 访问限频开启时，CDN 节点能针对单个 IP 的单位时间内的访问进行监控及统计，单个 IP 单位时间内的访问次数到达阀值时，CDN 节点返回状态码，并产生相关告警；
d) 应支持 IPv4 和 IPv6 地址。

7.4 UA 黑白名单

CDN 应支持 HTTP Header 字段 User-Agent 的识别及跟踪，并根据该字段制定规则实现访问控制，提升业务资源访问安全，具体要求如下：

a) CDN 应支持 UA 访问控制功能的开启及关闭；
b) CDN 能针对 UA 设置黑白名单访问控制策略，支持策略的增删改查；
c) 当用户访问到达 CDN 节点，CDN 能识别 UA 字段，并根据黑白名单策略判断是否返回对的请求资源，若 UA 字段命中黑名单访问策略，则直接返回状态码；若命中白名单访问策略，则返回请求资源。

8 内容防篡改

CDN 支持内容分发为了加速内容访问速度，需要在节点缓存源站内容，CDN 应能保障内容回源时、在节点间传输时、内容缓存到节点时以及内容从节点拉取时不被篡改：

a) CDN 支持内容回源防篡改，应能在回源时提供校验机制，保证内容一致性；
b) CDN 支持内容在节点间传输时不被篡改，应能在内容传输时提供校验机制，保证内容一致性；

c) CDN 支持内容缓存到节点不被篡改，应能提供检查机制，定时检测节点内容和源站内容的一致性；
d) CDN 支持内容从节点拉取时不被篡改，应能支持安全可靠传输协议。

9 内容合规

9.1 内容检测

9.1.1 内容安全审核系统集成

CDN 应有与第三方内容安全审核系统集成的能力，通过内容安全审核系统检测文本、图片、视频内容是否存在违法违规的异常内容。

9.1.2 内容异常检测

CDN 应满足以下内容异常检测要求：
a) CDN 支持通过第三方系统现有识别库，检测内容是否存在涉黄、涉欺、涉暴等异常；
b) CDN 支持内容异常存档，记录业务域名、URL、检测时间、异常截图等信息；
c) CDN 支持异常数据上报，通过开放接口支持对外上报异常，并记录上报状态及时间。

9.1.3 自定义检测

CDN 支持自定义识别库，客户可自定义不合规内容，系统能根据识别库内容识别到相关的图片、文本及视频。

9.2 异常内容管理

9.2.1 网站列表管理

CDN 应满足以下网站列表管理要求：
a) CDN 应具备对疑似违法违规网站列表的记录及更新能力，至少记录包含网站的域名、IP、违法违规类型、访问量、疑似违法违规发现时间、开始访问时间、最后访问时间、处理状态等信息；
b) CDN 支持实时更新网站列表；
c) CDN 应能支持疑似违法违规网站列表的长期保存及查询。

9.2.2 访问日志管理

CDN 支持网站的监管，具备 CDN 业务访问日志保存及查询的能力，具体要求如下：
a) CDN 应支持保存访问日志，日志信息至少包含访问 URL、源 IP、源端口、目的 IP、目的端口、访问时间；
b) CDN 应支持保存访问日志，保存周期可根据客户或监管部门的要求定义；
c) CDN 应支持访问日志查询，支持通过域名、时间段来查询日志，提供查询接口供监管部门进行调用；
d) CDN 应支持访问日志下载。

9.2.3 快速清除缓存

CDN 应具备以下快速清除缓存能力：
a) CDN 应支持在全网节点快速清除疑似违法违规内容的缓存；
b) CDN 应该具备隔离违法违规内容的能力，当发现有疑似违法违规内容时，隔离该内容防止该资源被重新访问。

9.2.4 监管系统对接

CDN应该能满足当地监管要求，具备广东省内、港澳地区信息安全管理系统的对接能力。

10 网络安全

10.1 安全防护

CDN 应支持 DDoS、WAF、BOT 安全防护，保障 CDN 业务不受各类网络攻击出现服务异常，具体要求如下：

a) CDN 支持 DDoS 攻击防护，应能支持网络层 DDoS 攻击防护，过滤 UDP Flood、SYN Flood、TCP Flood、ICMP Flood、ACK Flood、FIN Flood、RST Flood、DNS/NTP/SSDP 等反射攻击、空连接。支持应用层 DDoS 攻击防护，过滤 CC 攻击，支持 HTTP 自定义特征过滤如 HOST 过滤、User-agent 过滤、referer 过滤；

b) CDN 支持 WAF 攻击防护，应支持 web 攻击识别，有效防御常见 Web 攻击，如 SQL 注入、非授权访问、XSS 跨站脚本、CSRF 跨站请求伪造，Webshell 木马上传等 OWASP 定义的十大 Web 安全威胁攻击；

c) CDN 支持 BOT 防护，应支持有效防护公开类型 BOT 防护，包括搜索引擎、测速工具、内容聚合、扫描和网页爬虫等类别，可根据协议特征设置防护规则，包含 User-Agent 类别、HTTP 头部、HTTP 协议特征；

d) CDN 支持安全防护，应能支持防护策略配置以及防护统计报表。

10.2 安全告警

CDN 支持安全监控告警，通过告警及时发现 CDN 的安全状态并进行处理，具体要求如下：

a) CDN 支持告警规则定义，包含告警类型、告警条件以及频率等设置；

b) CDN 支持告警通知，包含短信、语音、电话等。

10.3 安全保护等级

在安全保护等级方面，CDN 应满足以下要求：

a) CDN 应支持网络安全合规，广东省内的 CDN 系统至少符合国家网络安全等级保护三级认证，需满足对应的安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全专家服务要求；

b) 港澳地区的 CDN 应至少符合 CSA STAR 二级安全认证，可选符合国家网络安全等级保护三级认证。

11 资源安全

11.1 资源覆盖

CDN 应满足以下资源覆盖要求：

a) CDN 应具备分布式节点资源覆盖能力。在广东省范围内，至少广州、深圳市内有覆盖节点，以保证用户访问广东省内本地覆盖率应不低于 90%。香港和澳门地区至少各有一个节点；

b) CDN 节点的建设应能满足业务加速的性能要求，保证页面加速能提升至少 30%、访问成功率大于 99%、首字节接收响应平均时间小于 2s、图片下载速率（640K）大于 700KB/s、图片（640K）下载耗时小于 2s、大文件（8M）下载速度大于 1200KB/s、大文件（8M）下载耗时小于 8s。

11.2 资源隔离

CDN 应满足以下资源隔离要求：

a) CDN 应支持使用专用加速节点，保证指定内容不被大规模加速缓存以防泄漏；

b) CDN 应能支持回源节点、区域中心节点、边缘节点的资源隔离；

c) CDN 应能支持隔离策略配置，指定域名、加速节点以及访问控制；

d) CDN 应能支持节点监测，提供访问日志。

11.3 资源合规

CDN 应满足以下资源合规要求：

a) CDN 节点建设应能保证资源安全可靠，节点资源采购应来自合规具备国内或港澳地区 IDC 经营许可的 IDC 机房与资源厂商；

b) 合规 IDC 能保障节点运行的可用性，同时具备完善的监控管理系统，保证物理资源的安全，避免缓存内容被非法窃取或篡改；
c) CDN 节点应能排查灰色节点资源接入，要求系统能监测节点资源状态，包含操作系统、CPU、内存、带宽等。

11.4 资源冗余

CDN 应满足以下资源冗余要求：

a) CDN 应支持调度系统、运营系统、边缘节点的冗余备份，在广东省、港澳地区至少支持有双系统备份，遇到故障可在规定时间内进行切换；
b) CDN 应支持核心系统链路冗余，支持多网络访问链路冗余备份，支持系统之间通信网络链路冗余备份；
c) CDN 应提供可服务的能力至少有 20%的冗余，可满足高峰期的业务请求。

参 考 文 献

[1] GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求
[2] CSA 0001-2016 云计算安全技术要求

.