

YDB

中国通信标准化协会标准

YDB 114—2012

互联网内容分发网络安全防护要求

Security Protection Requirements for Content Delivery Network over Internet

2012 - 11 - 13 印发

中国通信标准化协会

目 次

前言 III

1 范围 1

2 规范性引用文件 1

3 术语、定义和缩略语 1

 3.1 术语和定义 1

 3.2 缩略语 2

4 互联网内容分发网络安全防护概述 2

 4.1 互联网内容分发网络安全防护范围 2

 4.2 互联网内容分发网络安全风险分析 3

 4.3 互联网内容分发网络安全防护内容 4

5 互联网内容分发网络定级对象和安全等级确定 4

 5.1 社会影响力I 4

 5.2 规模和服务范围R 4

 5.3 所提供服务的的重要性V 4

6 互联网内容分发网络安全防护要求 5

 6.1 第1级要求 5

 6.2 第2级要求 5

 6.2.1 数据安全 5

 6.2.2 业务系统安全 5

 6.2.3 基础设施安全 7

 6.2.4 管理安全 8

 6.3 第3.1级要求 8

 6.3.1 数据安全 8

 6.3.2 业务系统安全 9

 6.3.3 基础设施安全 9

 6.3.4 管理安全 9

 6.4 第3.2级要求 10

 6.4.1 数据安全 10

 6.4.2 业务系统安全 10

 6.4.3 基础设施安全 11

 6.4.4 管理安全 11

 6.5 第4级要求 11

 6.6 第5级要求 11

附录A（资料性附录） 互联网内容分发网络风险分析 12

前 言

本标准是“电信网和互联网安全防护体系”系列标准之一。该系列标准预计结构及名称如下：

- 1、《电信网和互联网安全防护管理指南》；
- 2、《电信网和互联网安全等级保护实施指南》；
- 3、《电信网和互联网安全风险评估实施指南》；
- 4、《电信网和互联网灾难备份及恢复实施指南》；
- 5、《固定通信网安全防护要求》；
- 6、《移动通信网安全防护要求》；
- 7、《互联网安全防护要求》；
- 8、《增值业务网—消息网安全防护要求》；
- 9、《增值业务网—智能网安全防护要求》；
- 10、《接入网安全防护要求》；
- 11、《传送网安全防护要求》；
- 12、《IP承载网安全防护要求》；
- 13、《信令网安全防护要求》；
- 14、《同步网安全防护要求》；
- 15、《支撑网安全防护要求》；
- 16、《非核心生产单元安全防护要求》；
- 17、《电信网和互联网物理环境安全等级保护要求》；
- 18、《电信网和互联网管理安全等级保护要求》；
- 19、《固定通信网安全防护检测要求》；
- 20、《移动通信网安全防护检测要求》；
- 21、《互联网安全防护检测要求》；
- 22、《增值业务网—消息网安全防护检测要求》；
- 23、《增值业务网—智能网安全防护检测要求》；
- 24、《接入网安全防护检测要求》；
- 25、《传送网安全防护检测要求》；
- 26、《IP承载网安全防护检测要求》；
- 27、《信令网安全防护检测要求》；
- 28、《同步网安全防护检测要求》；
- 29、《支撑网安全防护检测要求》；
- 30、《非核心生产单元安全防护检测要求》；
- 31、《电信网和互联网物理环境安全等级保护检测要求》；
- 32、《电信网和互联网管理安全等级保护检测要求》；
- 33、《域名系统安全防护要求》；
- 34、《域名系统安全防护检测要求》；
- 35、《网上营业厅安全防护要求》；
- 36、《网上营业厅安全防护检测要求》；

- 37、《WAP网关系统安全防护要求》；
- 38、《WAP网关系统安全防护检测要求》；
- 39、《电信网和互联网信息服务业务系统安全防护要求》；
- 40、《电信网和互联网信息服务业务系统安全防护检测要求》；
- 41、《增值业务网 即时消息业务系统安全防护要求》；
- 42、《增值业务网 即时消息业务系统安全防护检测要求》；
- 43、《域名注册系统安全防护要求》；
- 44、《域名注册系统安全防护检测要求》；
- 45、《移动互联网应用商店安全防护要求》；
- 46、《移动互联网应用商店安全防护检测要求》；
- 47、《互联网内容分发网络安全防护要求》；
- 48、《互联网内容分发网络安全防护检测要求》；
- 49、《互联网数据中心安全防护要求》；
- 50、《互联网数据中心安全防护检测要求》。

本标准与YDB 115-2012《互联网内容分发网络安全防护检测要求》配套使用。

随着电信网和互联网的发展，将不断补充和完善电信网和互联网安全防护体系的相关标准。

为适应信息通信业发展对通信标准文件的需要，由中国通信标准化协会组织制定“中国通信标准化协会标准”，推荐有关方面参考采用。有关对本标准的建议和意见，向中国通信标准化协会反映。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：工业和信息化部电信研究院、蓝汛、网宿、清华大学、中国移动通信集团公司、中国电信集团公司、华为技术有限公司、中国互联网协会。

本标准主要起草人：魏薇、魏亮、谢玮、许会荃、于涛、魏凯、任巍、尹浩、陈伟、陈晓益、李金成、李增海。

互联网内容分发网络安全防护要求

1 范围

本标准规定了互联网内容分发网络安全等级的安全防护要求。
本标准适用于作为第三方对外提供互联网内容分发服务的网络。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是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 1754-2008 电信网和互联网物理环境安全防护要求

YD/T 1756-2008 电信网和互联网管理安全防护要求

YD/T 1746-2008 IP承载网安全防护要求

YDB 116-2012 互联网数据中心安全防护要求

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本标准。

3.1.1

互联网内容分发网络安全等级 security classification of CDN

互联网内容分发网络重要程度的表征。重要程度从互联网内容分发网络受到破坏后，对国家安全、社会秩序、经济运行、公共利益、网络和业务运营商造成的损害来衡量。

3.1.2

互联网内容分发网络安全等级保护 classified security protection of CDN

对互联网内容分发网络分等级实施安全保护。

3.1.3

互联网内容分发网络安全风险 security risk of CDN

人为或自然的威胁可能利用互联网内容分发网络中存在的脆弱性导致安全事件的发生及造成的影响。

3.1.4

互联网内容分发网络资产 asset of CDN

互联网内容分发网络中具有价值的资源，是安全防护体系保护的對象。互联网内容分发网络中的资产可能以多种形式存在，无形的、有形的、硬件、软件，包括物理布局、通信设备、物理线路、数据、软件、文档、规程、业务、人员、管理等各种类型的资源，如请求路由系统相关服务器。

3.1.5

互联网内容分发网络威胁 threat of CDN

可能导致对互联网内容分发网络产生危害的不希望事故潜在起因，它可能是人为的，也可能是非人为的；可能是无意失误，也可能是恶意攻击。

3.1.6

互联网内容分发网络脆弱性 vulnerability of CDN

互联网内容分发网络的资产中存在的弱点、缺陷与不足，不直接对互联网内容分发网络资产造成危害，但可能被互联网内容分发网络威胁所利用从而危害互联网内容分发网络资产的安全。

3.1.7

互联网内容分发网络灾难 disaster of CDN

由于各种原因，造成互联网内容分发网络故障或瘫痪，使互联网内容分发网络支持的业务功能停顿或服务水平不可接受、达到特定的时间的突发性事件。

3.1.8

互联网内容分发网络灾准备份 backup for disaster recovery of CDN

为了互联网内容分发网络灾难恢复而对相关网络要素进行备份的过程。

3.1.9

互联网内容分发网络灾难恢复 disaster recovery of CDN

为了将互联网内容分发网络从灾难造成的故障或瘫痪状态恢复到正常运行状态或部分正常运行状态、并将其支持的业务功能从灾难造成的不正常状态恢复到可接受状态，而设计的活动和流程。

3.1.10

互联网内容分发网络节点 node of CDN

简称CDN节点，在一个数据中心内部的CDN相关服务器组成一个CDN节点。

3.2 缩略语

下列缩略语适用于本标准。

CDN	Content Delivery Network over Internet	互联网内容分发网络
DDoS	Distributed Denial of Service	分布式拒绝服务
DoS	Denial of Service	拒绝服务
DNS	Domain Name System	域名系统

4 互联网内容分发网络安全防护概述

4.1 互联网内容分发网络安全防护范围

互联网内容分发网络CDN是指由一组相互联系、统一调度的内容缓存或加速节点组成的应用层网络，用于将内容从源站更有效地分发到互联网用户，以显著提高互联网用户的访问速度，改善互联网的拥塞状况，进而提升服务质量。互联网内容分发网络CDN可以分为企业自建自用的专用内容分发网、作为第三方对外提供服务的内容分发网。本标准仅对作为第三方对外提供互联网内容分发服务的CDN提出安全防护要求。

CDN位于内容源站与互联网用户之间，主要通过内容的分布式存储和就近服务提高内容分发的效率和服务质量，CDN是基于开放互联网的重叠网，与承载网松耦合，通常CDN内部由运营管理系统、请求路由系统、边缘服务器、监控系统组成，CDN外部与内容源站以及互联网用户相连，如图1所示。本标准的安全防护对象是CDN本身，不包含对内容源站的安全防护，承载网络的安全防护要求参见《IP承载网安全防护要求》，部署CDN服务器的IDC机房的安全防护要求参见《互联网数据中心安全防护要求》。

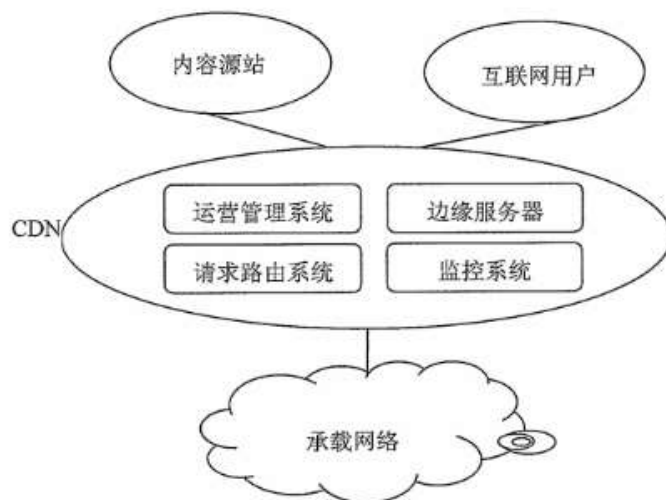


图1 互联网内容分发网络示意图

4.2 互联网内容分发网络安全风险分析

CDN中的重要资产至少应包括：

- CDN 关键业务系统及操作维护终端：如 CDN 中的运营管理系统、请求路由系统、边缘服务器、监控系统等涉及的服务器、数据库和操作维护终端；
- CDN 关键数据：如源站信息（IP 地址、域名、共享密钥等）、CDN 节点部署信息（CDN 在运营商的节点分布和带宽、内网部署、服务器的软件部署及调度、采集的策略等）、各业务系统服务器的管理口令和信息上传路径等。

CDN其他的资产（如文档、人员等）可参见附件1对资产的分类及举例。

CDN在内容源站与最终互联网用户之间增加了一层内容分发网，因此在CDN运营管理系统、请求路由系统、边缘服务器、监控系统的功能实现、部署、配置、管理等环节上均可能引入安全脆弱点。CDN面临来自公众互联网和内部网络的各种安全威胁，包括黑客发起DDOS攻击服务器或者篡改、重定向网站内容，不法分子窃取信息（如系统配置信息，互联网用户的Cookie、访问路径等），内部人员操作失误等。

CDN可能存在的安全脆弱性被利用后会产生很大的安全风险，例如：系统部署防入侵防攻击措施不到位，攻击者可能从外网渗透进内网系统；运营管理系统的数据配置操作失误，配置审计、保护措施不到位，信息可能被窃取或者被篡改；请求路由系统的域名解析安全机制存在脆弱性，可能出现CDN分发

的信息被劫持或重定向等安全事件；边缘服务器安全措施不到位，可能被DOS或DDOS攻击攻瘫；监控系统覆盖范围不够，无法及时发现和处理安全事件，或者内部人员利用提权篡改监控数据。这些安全隐患会对CDN的数据内容安全有效分发、业务正常提供构成安全威胁，甚至进一步威胁基础网络、内容源站和互联网用户终端的安全。

CDN的其他脆弱性和安全威胁可参见附件A的表A.2和表A.3。

4.3 互联网内容分发网络安全防护内容

CDN的主要功能是为互联网上的各种业务与应用提供内容分发服务，因此保障其分发的数据安全和CDN业务系统服务安全、防止信息被劫持或重定向、防止系统被攻击停止服务至关重要。保障CDN的基础设施安全、管理安全等也是安全防护的主要内容。

4.3.1 数据安全

主要包括数据一致性保护、安全审计、恶意数据清除、版权保护、备份数据安全等方面的安全要求。

4.3.2 业务系统安全

主要包括CDN的结构安全、访问控制、用户信息保护、攻击防范、入侵防范、请求路由系统安全以及冗余系统、冗余设备、冗余链路等方面的安全要求。

4.3.3 基础设施安全

主要包括主机安全、物理环境安全等方面的安全要求。

4.3.4 管理安全

主要包括机构、人员、制度等方面的安全要求。

5 互联网内容分发网络定级对象和安全等级确定

CDN的定级对象是作为第三方向网站等客户提供CDN服务的网络或系统。CDN运营企业应根据 YD/T 1729-2008附录A中确定安全等级的方法对其运营管理的CDN定级。针对各具体的CDN，可根据相应的社会影响力I、规模和服务范围R、所提供服务的的重要性V定级。建议权重值 α 、 β 、 γ 分别为：0.4、0.4、0.2，或者1/3、1/3、1/3，各CDN运营企业也可根据本企业实际情况调节 α 、 β 、 γ 三个权重值。

5.1 社会影响力 I

根据 YD/T 1729-2008，社会影响力表示定级对象受到破坏后对国家安全、社会秩序、经济运行、公共利益的损害程度。CDN服务对象可能是国家机关部委、企事业单位、企业网站等。建议服务于国家重要部委、国家级金融机构、国家级网络媒体等的CDN社会影响力赋值为4，服务于省级政府、地方金融机构、大型网站（如Alexa排名前50）等的CDN社会影响力赋值为3，服务于其他政府、企事业单位或一般网站等的CDN社会影响力赋值为2或1。

5.2 规模和服务范围 R

根据 YD/T 1729-2008，规模表示定级对象服务的用户数多少，服务范围表示定级对象服务的地区范围大小。建议从访问用户独立IP数、签约用户数、服务带宽等指标衡量CDN的规模和服务范围，例如，访问用户独立IP数月均达到5000万、或者签约用户数达到500个、或者服务带宽达到300G的CDN规模和服

务范围赋值为4,访问用户独立IP数月均达到3000万、或者签约用户数达到200个、或者服务带宽达到100G的CDN规模和服务范围赋值为3,其他CDN规模和服务范围赋值为2或1。

5.3 所提供服务的的重要性 V

根据 YD/T 1729-2008,所提供服务的的重要性表示定级对象提供的服务被破坏后对网络和业务运营商的合法权益的影响程度。CDN业务所提供服务的的重要性相对于基础运营商的传输、交换等业务重要性较低,相对于企业办公系统等业务所提供服务的的重要性高,建议CDN业务所提供服务的的重要性赋值为3或2。

6 互联网内容分发网络安全防护要求

6.1 第1级要求

不作要求。

6.2 第2级要求

6.2.1 数据安全

6.2.1.1 数据一致性保护

数据一致性保护要求如下:

- a) CDN运营企业应有能力保证CDN平台内部传输数据的一致性;
- b) CDN运营企业应具备分发的内容不被非法引用的能力,支持基于访问IP、时间、访问来源等方式的防盗链。

6.2.1.2 安全审计

安全审计要求如下:

- a) CDN系统应记录内容源站操作维护人员对其自主源站相关的CDN管理系统进行的管理操作和数据访问,日志记录保存至少60天,日志记录包含操作人员、操作时间、操作内容,操作结果等信息;
- b) CDN系统应记录CDN内部人员管理维护操作和数据访问,日志记录至少保留90天;
- c) CDN运营企业应对保存的操作日志定期(如每半年/季度/月审核一次)审计。

6.2.1.3 恶意数据清除

CDN运营企业应能在约定时间和范围内,根据国家或内容源站要求及时完成对被篡改页面或包含恶意代码页面(恶意代码可能内嵌在文本、图片、链接、可执行文件中)的屏蔽或清除操作,保证全网服务器屏蔽或清除全部恶意数据的系统完成时间在30分钟内。

6.2.2 业务系统安全

6.2.2.1 结构安全

结构安全要求如下:

- a) CDN运营企业应根据系统内部网络结构特点,按照统一的管理和控制原则划分不同的子网或网段,依照功能划分及重要性等因素分区部署相关设备;

- b) CDN 运营企业在节点部署时应考虑防范安全攻击, CDN 服务器单节点 (位于独立 IDC 机房内的 CDN 服务器群) 的服务能力 (如承载带宽量) 不超过全网的 20%;
- c) CDN 运营企业应采用多边缘服务器冗余配置抵抗攻击, 在一个边缘服务器受到攻击时, 可在规定时间内切换至冗余系统;
- d) CDN 的中央核心节点 (运营管理系统、请求路由系统、监控系统) 有实时备份节点, 可以在规定时间内切换至备份节点, 以保证服务的可持续性;
- e) CDN 运营企业在单个运营商内至少部署 3 个节点;
- f) CDN 运营企业应在软件结构上将各功能模块化, 从而实现对软件精细化管理, 一个软件的故障不影响其他软件提供服务;
- g) CDN 系统应具有安全监测能力、过滤攻击能力、容错能力、负载均衡调度能力;
- h) CDN 系统在运营过程中应具有抗攻击 (如 DDoS 攻击) 和快速恢复能力;
- i) CDN 系统应能隔离针对客户的安全攻击, 防止针对一个客户的攻击影响到其他客户。

6.2.2.2 访问控制

访问控制要求如下:

- a) CDN 系统应对内部操作维护管理人员进行身份认证;
- b) CDN 系统应对内容源站管理员的登录操作进行身份认证;
- c) CDN 系统的身份认证过程应通过 SSL 通道完成, 利用 SSH 安全登录;
- d) CDN 内部管理员应必须从公司内部 (包含外网 VPN 方式) 登陆 CDN 系统, CDN 系统通过用户密码、登录 IP 地址、黑白名单控制等进行访问限制;
- e) CDN 系统的操作维护管理员口令长度应不小于 8 字节, 口令应有复杂度要求 (使用大写字母、小写字母、数字、标点及特殊字符四种字符中至少二种的组合, 且与用户名或 ID 无相关性) 并定期更换 (更新周期不大于 90 天);
- f) CDN 系统应启用登录失败处理功能, 如限制非法登录次数、锁定账号等;
- g) CDN 系统对不同管理员的权限分级管理, 遵循权限最小分配原则, 管理权限不应超越该管理员的管辖范围。

6.2.2.3 用户信息保护

用户信息保护要求如下:

- a) CDN 系统应对 CDN 节点缓存的互联网用户信息 (如登录用户名、密码等) 进行加密保护, 采取有效措施防止用户信息被泄露、滥用;
- b) 未经内容源站允许, CDN 运营企业不得截获、存储互联网用户访问中的个人信息;
- c) CDN 系统加密保留 CDN 系统内部和内容源站操作维护人员的访问密码。

6.2.2.4 攻击防范

引入 CDN 后不应降低内容源站的安全水平, 同时 CDN 系统应提供对内容源站的抗攻击/压力保护, 包括但不限于抗 Synflood、UDPFlood、ACKFlood 等流量型 DDoS 攻击、承载访问压力等, 抗流量型 DDoS 攻击的能力不小于 500Mbps, 承载访问压力的能力不小于 3Gbps。

6.2.2.5 入侵防范

入侵防范要求如下:

- a) CDN 运营企业应采取安全措施 (如关闭不必要的端口和服务、限制访问地址) 防止 CDN 系统被入侵;

- b) CDN 运营企业应定期（每个月/季度/半年）对系统进行安全扫描和加固，检测 CDN 系统是否能够有效防范入侵、防篡改、防攻击、防病毒。

6.2.2.6 请求路由系统安全

请求路由系统安全要求如下：

- a) CDN 运营企业在全国至少部署两个 DNS 节点进行冗余备份；
- b) CDN 运营企业应尽可能采用包含最新补丁的 DNS 服务器软件；
- c) CDN 运营企业应参照《域名系统安全防护要求》对 DNS 服务器进行与所在互联网内容分发网络相同级别的安全设置。

6.2.2.7 冗余系统、冗余设备及冗余链路

冗余系统、冗余设备及冗余链路要求如下：

- a) CDN 系统应进行冗余配置，为多个边缘节点提供安全可靠稳定的服务，运营管理系统、请求路由系统应有至少两个备份系统，部署于多个省份，在遇到故障和攻击时应能在 30 分钟内完成系统切换；
- b) CDN 系统中所有设备的处理能力应具备至少 20% 的冗余，能够满足业务高峰期需要；
- c) CDN 系统的核心系统（请求路由系统、运营管理系统、监控系统）有专有链路接入相关运营商，每个节点上联接入有备份光纤；
- d) CDN 系统的核心系统（请求路由系统、运营管理系统、监控系统）间通过多链路相连。

6.2.3 基础设施安全

6.2.3.1 主机安全

6.2.3.1.1 访问控制

访问控制要求如下：

- a) CDN 系统应对登录操作系统和数据库系统的用户进行身份标识和鉴别；
- b) CDN 系统应为操作系统和数据库系统的不同用户分配不同的用户名，确保用户名具有唯一性；
- c) 操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，相关用户口令长度应不小于 6 字节，口令应有复杂度要求（使用大写字母、小写字母、数字、标点及特殊字符四种字符中至少二种的组合，且与用户名或 ID 无相关性）并定期更换（更新周期不大于 90 天）；
- d) CDN 系统应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；
- e) 当对各类主机进行远程管理时，CDN 系统应采取保护措施（如使用加密协议）防止鉴别信息在传输过程中被窃听；
- f) CDN 系统应启用访问控制机制或策略，依据安全策略控制操作维护人员对资源的访问；
- g) CDN 运营企业应及时删除多余的、过期的帐户，避免共享帐户的存在；
- h) CDN 运营企业应实现操作系统和数据库系统特权用户的权限分离；
- i) CDN 运营企业应限制默认帐户的访问权限，修改这些帐户的默认口令，设备功能配置可更改的情况下，应重命名默认帐户。

6.2.3.1.2 安全审计

安全审计要求如下：

- a) 审计范围应覆盖到主机/服务器上的每个操作系统用户和数据库用户；

- b) 审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件;
- c) 审计记录应包括事件的操作人员、操作对象、操作内容、操作时间和操作结果等;
- d) CDN 运营企业应保护审计记录, 避免其受到未预期的删除、修改或覆盖等, 保留一定期限 (至少 180 天)。

6.2.3.1.3 入侵防范

操作系统应遵循最小安装的原则, 仅安装需要的组件和应用程序, 并通过安全的方式 (如设置升级服务器) 保持系统补丁及时得到更新。

6.2.3.1.4 资源控制

资源控制要求如下:

- a) CDN 运营企业应对边缘服务器、核心系统 (请求路由系统、运营管理系统、监控系统) 进行性能监测, 包括监测服务器的 CPU、硬盘、内存、网络等资源的使用情况;
- b) CDN 运营企业应能够对服务器、数据库等系统的服务水平设定告警阈值, 当监测到服务水平降低到阈值时应能进行告警。

6.2.3.2 物理环境安全

应满足 YD/T 1754-2008 中要求。

6.2.4 管理安全

应满足 YD/T 1756-2008 中第 2 级的相关要求。此外, 还应满足如下要求:

- a) CDN 运营企业应要求员工需经过培训并通过考核才能上岗;
- b) CDN 运营企业应为内容源站提供 7X24 技术支持;
- c) CDN 运营企业应有专职的安全管理责任人;
- d) 监控人员应能够及时发现安全攻击和系统当机等异常事件, 并在企业规定时间内汇报运维人员、管理人员和公司核心管理人员, 同时在规定时间内通知内部客户服务人员;
- e) 运维人员应根据安全事件及时启动系统安全预案, 及时跟进安全事件解决情况, 及时向上级汇报;
- f) 客服人员应能及时 (按照服务协议条款) 向客户 (即内容源站) 反馈问题解决建议和对策, 协调客户完成相应部署和测试;
- g) CDN 运营企业应针对各类安全攻击 (如 CDN 遭受 DDOS 攻击, 请求路由系统遭受攻击, 域名污染或者内容污染, 节点故障或者带宽服务质量不能接受, 核心数据遭到破坏等) 准备详细的应急处理预案;
- h) CDN 运营企业应对 CDN 全网系统有 7X24 小时监控;
- i) CDN 运营企业针对灾难的服务恢复时间应满足企业要求 (按照服务协议条款);
- j) CDN 运营企业应对灾难恢复预案进行教育、培训和演练。

6.3 第 3.1 级要求

6.3.1 数据安全

6.3.1.1 数据一致性保护

除满足第 2 级的要求之外, CDN 运营企业还应有能力保证 CDN 数据与内容源站传输的一致性。

6.3.1.2 安全审计

同2级要求。

6.3.1.3 恶意数据清除

除满足第2级的要求之外，CDN运营企业还应能在国家相关部门或内容源站方要求时间和范围内，及时完成对被篡改页面或包含恶意代码页面（恶意代码可能内嵌在文本、图片、链接、可执行文件中等）的屏蔽或清除操作，保证全网服务器屏蔽或清除全部恶意数据的系统完成时间在15分钟内。

6.3.1.4 版权保护

除满足第2级的要求之外，还应满足：

- a) CDN运营企业应与内容源站商定具体的版权保护措施和方法，共同实现版权保护。CDN系统应按照内容源站的要求提供内容鉴权、用户鉴权、IP地址鉴权、使用终端鉴别以及组合鉴权；
- b) CDN系统应提供对公开版权保护技术的支持；
- c) CDN系统应支持客户定制的内容保护技术和内容解密途径；
- d) CDN系统应支持基于用户身份验证（包括回源站认证或者CDN代验证）的版权保护；
- e) CDN系统应支持基于用户访问的时间特性进行认证；
- f) CDN系统应支持基于用户使用的IP地址进行访问限制。

6.3.1.5 备份数据安全

除满足第2级的要求之外，还应满足：

- a) CDN运营企业应在多个核心节点备份配置管理系统的系统管理数据，应每30分钟同步一次；
- b) CDN运营企业应对源站托管数据进行多点容灾备份，应在30分钟完成数据同步。

6.3.2 业务系统安全

6.3.2.1 结构安全

除满足第2级的要求之外，还应满足CDN运营企业在单个运营商内至少部署10个节点。

6.3.2.2 访问控制

同第2级要求。

6.3.2.3 用户信息保护

同第2级要求。

6.3.2.4 攻击防范

除满足第2级的要求之外，还应满足：

- a) 引入CDN后不应降低内容源站的安全水平，同时CDN系统应提供对内容源站的抗攻击/压力保护，包括不限于抗Synflood、UDPFlood、ACKFlood等流量型DDOS攻击，承载访问压力等，抗流量型DDOS攻击的能力不小于2Gbps，承载访问压力的能力不小于10Gbps；
- b) 当攻击量或访问压力超过CDN的承载能力，CDN运营企业应能够采取有效措施避免造成CDN网络的全面瘫痪。

6.3.2.5 入侵防范

同第2级要求。

6.3.2.6 请求路由系统安全

除满足第2级的要求之外，还应满足：

- a) DNS 服务解析具有抗攻击能力，支持 DNS 系统监控、DNS 可用性（外部可访问）监控、DNS 防攻击等；
- b) DNS 可处理整个系统的历史访问量采样集的 95th 百分点的 3 倍访问量；
- c) 全国至少部署三个请求路由系统节点进行冗余备份。

6.3.2.7 冗余系统、冗余设备及冗余链路

同第2级要求。

6.3.3 基础设施安全

同第2级要求。

6.3.4 管理安全

应满足第2级、YD/T 1756-2008中第3.1级的相关要求。

6.4 第3.2级要求

6.4.1 数据安全

6.4.1.1 数据一致性保护

除满足第3.1级的要求之外，CDN运营企业还应具有防止CDN边缘服务器回源站域名解析遭到劫持的能力和措施，在源站配合下CDN的边缘服务器能避免受到公网DNS的污染或者劫持进而向错误的源站发出内容请求。

6.4.1.2 安全审计

同3.1级要求。

6.4.1.3 恶意数据清除

除满足第3.1级的要求之外，CDN运营企业还应能够在国家或内容源站要求时间和范围内，及时完成对被篡改页面或包含恶意代码页面（恶意代码可能内嵌在文本、图片、链接、可执行文件中）的屏蔽或清除操作，保证全网服务器屏蔽或清除全部恶意数据的系统完成时间在10分钟内。

6.4.1.4 版权保护

除满足第3.1级的要求之外，CDN运营企业还应针对不同类型终端（机顶盒、手机、PC等）均提供版权保护。

6.4.1.5 备份数据安全

除满足第3.1级的要求之外，还应满足：

- a) CDN 运营企业应在多个核心节点备份运营管理系统的管理数据，应每 10 分钟同步一次；
- b) CDN 运营企业应对源站托管数据进行多点容灾备份，应在 10 分钟完成数据同步。

6.4.2 业务系统安全

6.4.2.1 结构安全

同第3.1级要求。

6.4.2.2 访问控制

除满足第3.1级的要求之外，还应满足CDN系统可为源站客户分配多个账号，并根据管理身份及权限赋予相应的访问权限。

6.4.2.3 用户信息保护

同第3.1级要求。

6.4.2.4 攻击防范

同第3.1级要求。

6.4.2.5 入侵防范

同第3.1级要求。

6.4.2.6 请求路由系统安全

除满足第3.1级的要求之外，CDN的DNS服务还应根据国家相关要求在相应部门注册，CDN运营企业承担相应的管理责任，根据国家要求完成紧急事件处理。

6.4.2.7 冗余系统、冗余设备及冗余链路

除满足第3.1级的要求之外，CDN系统的请求路由系统、配置管理系统还应有多份（至少四份）备份系统，在遇到故障和攻击时能无缝完成系统切换。

6.4.3 基础设施安全

同第3.1级要求。

6.4.4 管理安全

应满足第3.1级、YD/T 1756-2008中第3.2级的相关要求。此外，还应满足：

- a) CDN运营企业应对相关管理和技术人员定期（每个月或每个季度）组织安全技术培训和考核；
- b) CDN运营企业应定期（每个月或者每个季度）组织对灾难恢复预案的教育、培训和演练。

6.5 第4级要求

同3.2级要求。

6.6 第5级要求

待补充。

附 录 A
(资料性附录)
互联网内容分发网络风险分析

本附录指导互联网内容分发网络风险分析过程中的资产、脆弱性、威胁分析。
CDN的资产至少应包括：设备软硬件，重要数据，文档，人员等，如表A.1所示。

表A.1 资产列表

分类	主要资产
设备及链路	请求路由系统、边缘服务器、运营管理系统、监控系统等涉及的操作维护终端、服务器和数据库，系统内部网络设备（如，系统内部组网路由器、交换机等设备）、系统内部链路。
数据和信息	保证 CDN 正常提供业务的数据和信息（如，业务数据、系统配置数据、管理员操作维护记录、用户信息等）； CDN 比较重要的数据包括：与客户相关的源站信息（IP 地址、域名、共享密钥等）、CDN 节点部署信息（CDN 在运营商的节点分布、带宽和内网分布、服务器的软件部署及调度、采集的策略和应对方案等）、服务器的管理口令、服务器的信息上传路径等
文档和资料	纸质以及保存在存储介质中的各种文件资料（如，设计文档、技术要求、管理规定、工作计划、技术报告、用户手册等）；
人员	相关管理、维护、开发、数据备份人员等。
环境和设施	业务系统和设备所处的物理环境，机房、电力、防火、防水、防静电、温湿度控制等相关设施。

表A.2列举出互联网内容分发网络的主要的脆弱性识别内容。

表A.2 脆弱性分析表

类型	对象	存在的主要脆弱性
技术脆弱性	业务及应用	CDN 的 DNS 系统内置安全机制脆弱 相关服务器未进行合理备份，重要数据未及时进行备份； 相关业务存在漏洞，相关服务器的应用代码存在漏洞、后门； 相关服务器存在过多不必要的开放端口； 相关服务器配置不合理，访问控制策略设置不合理； 相关服务器的日志功能没有启用或不够详细； 系统规划、设备部署、链路部署、资源配置、业务保护和恢复能力、安全技术措施和策略等方面的缺陷；
	设备	相关设备存在硬件隐患或质量问题； 相关设备的操作系统存在安全隐患； 相关口令设置不合理、复杂度不够、或没有经常更新； 设备重要部件未进行合理备份； 相关设备超过使用年限或核心部件老化； 相关设备发生故障后未及时告警；
	物理环境	机房地选择不合理； 防火、供配电、防静电、接地与防雷、电磁防护、温湿度控制不符合规范； 通信线路、相关服务器、主机等设备的保护不符合规范；

表 A.2 (续)

类型	对象	存在的主要脆弱性
管理脆弱性		<p>安全管理机构方面：岗位设置不合理（如人员配置过少、职责不清）、授权和审批程序简化、沟通和合作未执行、审核和检查未执行等；</p> <p>安全管理制度方面：管理制度不完善、制度评审和修订不及时等；</p> <p>人员安全管理方面：人员录用不符合程序、人员离岗未办理安全手续、人员未进行安全培训、对于第三方人员未进行限制访问等；</p> <p>建设管理方面：安全方案不完善、软件开发不符合程序、工程实施未进行安全验收或验收不严格等；</p> <p>运维管理方面：物理环境管理措施简单、存储介质使用不受限、设备没有定期维护、厂家支持力度不够、关键性能指标没有定期监控、无恶意代码防范措施、无数据备份和恢复策略、访问控制不严格、操作管理不规范等，应急保障措施不到位，灾难恢复预案不完善。</p>

CDN安全威胁可分为技术威胁、环境威胁和人为威胁。环境威胁包括自然界不可抗的威胁和其它物理威胁。根据威胁的动机，人为威胁又可分为恶意和非恶意两种。表A.3列举出CDN主要面临的威胁。

表A.3 威胁来源列表

来源		主要威胁描述
环境威胁	物理环境	断电、静电、灰尘、潮湿、温湿度异常、电磁干扰等； 意外事故或通讯线路方面的故障；
	自然灾害	鼠蚁虫害、洪灾、火灾、泥石流、山体滑坡、地震、台风、雷击；
人为威胁	恶意人员	<p>不满的或有预谋的内部人员滥用权限进行恶意破坏；</p> <p>攻击者利用非法手段进入机房内部盗窃、破坏、篡改源站内容，攻击者非法物理访问相关设备、存储介质等；</p> <p>攻击者利用网络协议、操作系统、应用系统漏洞，越权访问相关设备的文件、数据或其他资源；</p> <p>攻击者利用各种工具获取相关设备身份鉴别数据，并对鉴别数据进行分析和解剖，获得鉴别信息，未授权访问应用系统，或非法使用相关文件和数据；</p> <p>攻击者利用应用系统扩散病毒、蠕虫，利用相关攻击工具恶意消耗应用系统资源（如发动DNS攻击、DDoS），导致系统能力下降或瘫痪、无法正常提供应用服务；</p> <p>攻击者截获数据，进行篡改、插入，并重发，造成数据的完整性、真实性丧失；</p>
	无恶意人员	<p>内部人员由于缺乏责任心或者无作为，应该执行而没有执行相应的操作、或无意地执行了错误或危险的操作导致安全事件；</p> <p>内部人员没有遵循规章制度和操作流程而导致故障或信息损坏；内部人员由于缺乏培训、专业技能不足、不具备岗位技能要求而导致故障或攻击；</p> <p>安全管理制度不完善、落实不到位造成安全管理不规范或者管理混乱导致安全事件；</p> <p>内部人员由于安全检查不及时不到位导致CDN主机和服务器、及系统网络设备使用时间过长或质量问题等导致硬件故障，系统链路发生故障，相关设备的操作系统软件、应用软件运行故障，相关设备数据丢失或系统运行中断，存储介质老化或质量问题等导致不可用，CDN的DNS系统内置安全机制脆弱导致CDN可能遭到缓存感染、信息劫持、重定向等攻击，CDN不能正常运行。</p>

中国通信标准化协会标准
互联网内容分发网络安全防护要求
YDB 114-2012

*

版权所有 不得翻印

中国通信标准化协会标准化推进中心承办印发
地址：北京新街口外大街 28 号
邮编：100088
电话：010-82058764 010-82054513
电子版发行网址：www.ptsnet.cn