



中华人民共和国国家标准

GB/T 45279.4—2025

IPv4/IPv6 网络安全防护技术规范 第4部分：内容分发网络

IPv4/IPv6 network security protection technical specifications—
Part 4: Content delivery network

2025-02-28 发布

2025-06-01 实施

国家市场监督管理总局
国家标准化管理委员会 发布

目 次

前言 III

引言 IV

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 缩略语 1

5 CDN 总体要求 2

 5.1 CDN 安全防护范围 2

 5.2 CDN 安全防护内容 2

6 CDN 安全防护要求 2

 6.1 第 2 级要求 3

 6.2 第 3 级要求 6

7 CDN 安全防护测试方法 7

 7.1 第 2 级测试方法 7

 7.2 第 3 级测试方法 18

参考文献 24



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。

GB/T 45279《IPv4/IPv6 网络安全防护技术规范》与 GB/T 44810《IPv6 网络安全设备技术要求》共同构成支撑 IPv6 安全的国家标准体系。

本文件是 GB/T 45279《IPv4/IPv6 网络安全防护技术规范》的第 4 部分。GB/T 45279 已经发布了以下部分：

- 第 1 部分：IP 承载网；
- 第 2 部分：移动通信网；
- 第 3 部分：互联网数据中心；
- 第 4 部分：内容分发网络。

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。

本文件由中华人民共和国工业和信息化部提出。

本文件由全国通信标准化技术委员会(SAC/TC 485)归口。

本文件起草单位：中国信息通信研究院、网宿科技股份有限公司、中兴通讯股份有限公司、阿里云计算有限公司、中国信息通信科技集团有限公司、国家计算机网络应急技术处理协调中心。

本文件主要起草人：孟楠、贺倩、温国洲、翁志真、王魏强、张晓渠、李克、杨阔、曾斌、王健、雷君、严定宇。

引 言

根据《关于加快推进互联网协议第六版(IPv6)规模部署和应用工作的通知》,为更好面对网络复杂化和用户规模扩大化带来的安全挑战,推动 IPv6 网络安全工作的标准化,我国制定了一系列 IPv6 安全标准。其中,GB/T 45279《IPv4/IPv6 网络安全防护技术规范》是为规范电信网和互联网重要网络单元在 IPv6 部署后所开展的安全防护工作,拟分为以下部分。

- 第 1 部分:IP 承载网。目的在于 IPv6 部署后,推动 IP 承载网的安全防护工作。
- 第 2 部分:移动通信网。目的在于 IPv6 部署后,推动移动通信网的安全防护工作。
- 第 3 部分:互联网数据中心。目的在于 IPv6 部署后,推动互联网数据中心的安全防护工作。
- 第 4 部分:内容分发网络。目的在于 IPv6 部署后,推动内容分发网络的安全防护工作。



IPv4/IPv6 网络安全防护技术规范

第 4 部分:内容分发网络

1 范围

本文件规定了 IPv4、IPv6、双栈环境下作为第三方对外提供内容分发服务的内容分发网络(CDN)的安全防护要求和测试方法,包括数据安全、业务系统安全、主机安全、物理环境安全和管理安全等方面。

本文件适用于指导支持 IPv4/IPv6 协议的 CDN 安全防护工作开展和推进。

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。

GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求
GB/T 22240—2020 信息安全技术 网络安全等级保护定级指南
YD/T 2052—2015 域名系统安全防护要求
YD/T 3799—2020 电信网和互联网网络安全防护定级备案实施指南

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; CDN

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。

3.2

CDN 节点 node of CDN

CDN 通过统一的资源管理和调度管理的分布在不同区域的服务器。

注:以下简称为“节点”。

4 缩略语

下列缩略语适用于本文件。

CDN:内容分发网络(Content Delivery Network)
DDoS:分布式拒绝服务(Distributed Denial of Service)
DNS:域名系统(Domain Name System)
IP:网际协议(Internet Protocol)
IPv4:互联网协议第四版(Internet Protocol Version 4)
IPv6:互联网协议第六版(Internet Protocol Version 6)
SSL:安全套接层(Secure Socket Layer)

UDP:用户数据包协议(User Datagram Protocol)

VPN:虚拟专用网络(Virtual Private Network)

5 CDN 总体要求

5.1 CDN 安全防护范围

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、DNS 调度系统、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。本文件的安全防护对象是 CDN 本身,不包含对内容源站的安全防护、承载网络安全防护要求和部署以及 CDN 服务器的 IDC 机房的安全防护要求,其应遵循各自防护要求标准。

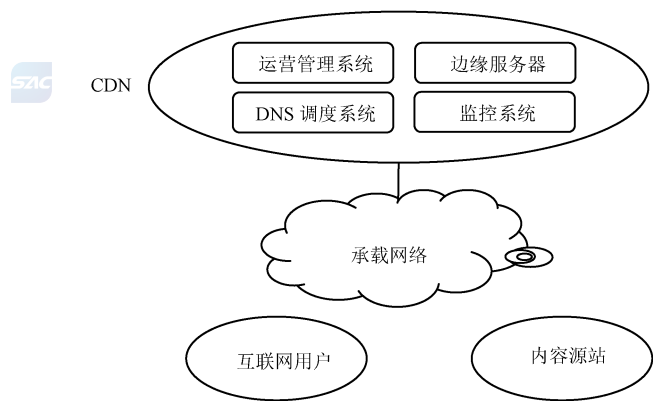


图 1 内容分发网络示意图

5.2 CDN 安全防护内容

应按照 GB/T 22240—2020、YD/T 3799—2020 确定移动通信网符合的安全等级,并在遵循 GB/T 22239—2019 规定的相应安全等级安全通用要求基础上,按照本文件要求开展包括数据安全、业务系统安全、主机安全、物理环境安全和管理安全等五个层面的安全防护工作。本文件提出第 2 级和第 3 级要求,第 4 级、第 5 级要求暂同第 3 级要求。其中:

- a) 数据安全:主要包括 CDN 的数据一致性保护、安全审计、恶意数据清除等方面内容和要求;
- b) 业务系统安全:主要包括 CDN 的结构安全、访问控制安全、攻击和入侵防范等方面的内容和要求;
- c) 主机安全:主要包括 CDN 的主机访问控制、安全审计、入侵防范等方面内容和要求;
- d) 物理环境安全:主要包括 CDN 所在的物理环境的安全要求;
- e) 管理安全:主要包括 CDN 的安全管理、风险评估、应急预案等方面内容和要求。

6 CDN 安全防护要求

6.1 第 2 级要求

6.1.1 数据安全

6.1.1.1 数据一致性保护

数据一致性保护满足以下要求:

- a) CDN 系统应保证内部传输数据的一致性,支持基于加密传输等方式确保 CDN 系统内部传输

数据的一致性；

- b) CDN 系统应具备分发的内容不被非法引用的能力,支持基于访问来源 IP、时间、地域、加密签名等方式的防盗链；
- c) CDN 系统应能检测并及时阻断缓存页面在传输过程中非法广告及非法内容、数据的插入。

6.1.1.2 安全审计

数据安全审计满足以下要求：

- 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 180 d,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 180 d；
- c) 保存的操作日志应定期(如每半年/季度/月)进行审计。

6.1.1.3 恶意数据清除

CDN 系统应根据国家有关部门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 30 min 内。

6.1.2 业务系统安全

6.1.2.1 结构安全

业务系统结构安全满足以下要求：

- a) CDN 系统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 系统应做好内外网隔离,内部 IPv4 地址、IPv6 全局地址应拒绝外网直接访问；
- c) CDN 系统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%；
- d) CDN 系统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；
- e) CDN 的中央核心节点(运营管理系统、DNS 调度系统、监控系统)有实时备份节点,可在规定时间内切换至备份节点,以保证服务的可持续性；
- f) CDN 系统在单个运营商内至少部署 3 个节点；
- g) CDN 系统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；
- h) CDN 系统应具有较为完备的 IPv4/IPv6 安全防护能力,包括安全监测能力、过滤攻击能力、容错能力、负载均衡调度能力,能够防护 IPv4/IPv6 网络环境下主流的 Web 应用攻击,例如 OWASP 排名前十的 Web 应用程序漏洞等；
- i) CDN 系统应具有抗攻击(如 DDoS 攻击)和快速恢复能力；
- j) CDN 系统应具备隔离针对单一客户攻击的能力,防止或降低攻击对其他客户的影响。

6.1.2.2 访问控制

业务系统访问控制满足以下要求：

- 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；



- d) CDN 内部管理员应从内部网络(或外网 VPN 方式)登录 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 2 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 d);
- 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;
- h) CDN 系统应具备 IPv4/IPv6 地址的访问控制能力。

6.1.2.3 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 IPv4/IPv6 网络下的抗攻击/压力保护,包括抗同步泛洪攻击、UDP 泛洪攻击等流量型 DDoS 攻击、承载访问压力等,抗流量型 DDoS 攻击的能力不小于 600 Gbit/s,承载访问压力的能力不小于 3 Gbit/s。

6.1.2.4 入侵防范

业务系统入侵防范满足以下要求:

- a) CDN 系统应采取安全措施(如 ACL 中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 系统应定期(每月/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入侵。

6.1.2.5 DNS 调度系统安全

CDN 系统的 DNS 调度系统安全满足以下要求:

- a) CDN 系统的 DNS 调度系统应支持 IPv4/IPv6 协议;
- b) CDN 系统的 DNS 调度系统应采用最新版本的 DNS 服务器软件;
- c) CDN 系统的 DNS 调度系统应与所在 CDN 系统具有相同的安全等级,并按照 YD/T 2052—2015 中 5.1~5.3 的安全要求开展与安全等级相应的安全防护工作。

6.1.2.6 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满足以下要求:

- 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、DNS 调度系统等 CDN 系统的核心系统均应至少有两个备份系统(宜部署在不同省份),保证系统在遇到故障和攻击时应能在 30 min 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(DNS 调度系统、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(DNS 调度系统、运营管理系统、监控系统)间通过多链路相连。

6.1.3 主机安全

6.1.3.1 访问控制



主机访问控制满足以下要求:

- 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8位,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2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 d);
- 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系统应及时删除多余的、过期的账户,避免共享账户的存在;
- h) CDN系统应实现操作系统和数据库系统特权用户的权限分离;
- i) CDN系统应限制默认账户的访问权限,修改这些账户的默认口令,设备功能配置可更改的情况下,应重命名默认账户;
- j) CDN系统应根据会话状态信息为数据流提供明确的允许/拒绝访问的能力,控制粒度到主机级。

6.1.3.2 安全审计

主机安全审计满足以下要求:

- 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系统应保护审计记录,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 d)。

6.1.3.3 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。主机和网络层面均应部署防入侵、防病毒软件或者硬件。

6.1.3.4 资源控制

主机资源控制满足以下要求:

- a) CDN系统应对边缘服务器、核心系统(DNS调度系统、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系统应能够对服务器、数据库等系统的服务水平设定告警阈值,当监测到服务水平指标触发阈值时应能进行告警。

6.1.4 物理环境安全

应满足GB/T 22239—2019中第二级的安全物理环境要求。

6.1.5 管理安全

除满足GB/T 22239—2019中第二级的安全管理制度、安全管理机构、安全管理人员、安全运维管理相关要求外,还满足以下要求:

- a) 监控人员应能够及时发现安全攻击和系统宕机等异常事件,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;
- b) 运维人员应能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；

- c) 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 and 对策,协调客户完成相应部署和测试；
- d) CDN 系统应针对各类安全攻击(如 CDN 遭受 DDoS 攻击,DNS 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；
- e) CDN 系统应对 CDN 全网系统有 7×24 h 监控；
- f) CDN 系统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)；
- g) CDN 系统应对灾难恢复预案进行教育、培训和演练。

6.2 第 3 级要求

6.2.1 数据安全

6.2.1.1 数据一致性保护

除满足第 2 级的要求之外,还满足以下要求：

- a) CDN 系统应有能力保证 CDN 数据与内容源站传输的一致性,支持 MD5 值比对、Etag 值比对等方式保证 CDN 数据与内容源站传输的一致性；
- b) CDN 系统应具有防止 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。

6.2.1.2 安全审计

除满足第 2 级的要求之外,还满足以下要求：

应具有对审计记录数据进行统计、查询、分析及生成审计报表的功能。

6.2.1.3 恶意数据清除

CDN 系统应能够在国家相关部门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 10 min 内。

6.2.1.4 备份数据安全

备份数据安全满足以下要求：

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

6.2.2 业务系统安全

6.2.2.1 结构安全

除满足第 2 级的要求之外,还应满足以下要求：

CDN 系统在单个运营商内至少部署 10 个节点。

6.2.2.2 访问控制

除满足第 2 级的要求之外,还满足以下要求：

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。

6.2.2.3 攻击防范

除满足第2级的要求之外,还满足以下要求:

- 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IPv4/IPv6网络下的抗攻击/压力保护,包括抗同步泛洪攻击、UDP泛洪攻击等流量型DDoS攻击,承载访问压力等,抗流量型DDoS攻击的能力不小于1.2 Tbit/s,承载访问压力的能力不小于10 Gbit/s;
- b) 当攻击量或访问压力超过CDN的承载能力,CDN系统应能够采取有效措施避免造成CDN网络的全面瘫痪。

6.2.2.4 入侵防范

同第2级要求。

6.2.2.5 DNS调度系统安全

除满足第2级的要求之外,还满足以下要求:

- 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攻击等;
- b) DNS可处理整个系统的96 h内历史访问量采样集的3倍访问量;
- c) CDN的DNS服务应根据国家相关要求在相应部门注册。

6.2.2.6 冗余系统、冗余设备及冗余链路

除满足第2级的要求之外,还满足以下要求:

CDN系统的DNS调度系统、配置管理系统应有多份(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。

6.2.3 主机安全

同第2级要求。

6.2.4 物理环境安全

应满足GB/T 22239—2019中第三级的安全物理环境要求。

6.2.5 管理安全

应满足第2级以及GB/T 22239—2019中第三级的安全管理制度、安全管理机构、安全管理人员、安全运维管理相关要求。

7 CDN安全防护测试方法

7.1 第2级测试方法

7.1.1 数据安全

7.1.1.1 数据一致性保护

第2级数据一致性保护的测试方法见表1~表3。

表 1 数据一致性保护 2 级内部传输数据测试方法

测试编号:CDN-第 2 级-数据安全-数据一致性保护-01
测试项目:6.1.1.1a)CDN 系统应保证内部传输数据的一致性,支持基于加密传输等方式确保 CDN 系统内部传输数据的一致性
测试步骤: 1) 访谈 CDN 运营企业是否有能力保证 CDN 平台内部传输数据一致性,是否支持基于加密传输方式确保 CDN 平台内部传输数据的一致性; 2) 测试者提供一个源站,被测试者提供两级缓存服务器,测试者向边缘缓存服务器请求测试的 URL,在传输过程中测试者篡改两个缓存服务器之间传输的数据,测试者应无法获得被篡改的数据; 3) 清除缓存,测试者再次向边缘缓存服务器请求同样的 URL,不执行篡改操作,测试者得到结果后与源站内容对比
预期结果: CDN 系统应保证内部传输数据的一致性
判定原则: 达到以上预期结果,则通过,否则不通过

表 2 数据一致性保护 2 级非法引用测试方法

测试编号:CDN-第 2 级-数据安全-数据一致性保护-02
测试项目:6.1.1.1b)CDN 系统应具备分发的内容不被非法引用的能力,支持基于访问来源 IP、时间、地域、加密签名等方式的防盗链
测试步骤: 1) 访谈 CDN 运营企业是否有能力保护分发的内容不被非法引用; 2) CDN 对访问链接进行来源防盗链配置,测试人员通过其他网站引用该链接; 3) CDN 对链接进行访问 IP 防盗链配置,测试人员通过不在设置 IP 范围内的 IP 地址访问该内容; 4) CDN 对链接进行访问 IP 防盗链配置,测试人员通过在 IP 范围内的 IP 地址访问; 5) CDN 进行访问时间防盗链配置,测试人员在配置时间外访问; 6) CDN 进行访问时间防盗链配置,在配置时间内访问
预期结果: CDN 系统应具备分发的内容不被非法引用的能力,支持基于访问来源 IP、时间、地域、加密签名等方式的防盗链
判定原则: 达到以上预期结果,则通过,否则不通过

表 3 数据一致性保护 2 级数据阻断测试方法

测试编号:CDN-第 2 级-数据安全-数据一致性保护-03
测试项目:6.1.1.1c)CDN 系统应能检测并及时阻断缓存页面在传输过程中非法广告及非法内容、数据的插入
测试步骤: 测试者通过缓存服务器请求测试的 URL,在传输过程中测试者篡改源站与缓存服务器之间传输的数据,插入恶意链接或者非法内容
预期结果: CDN 系统应能检测并及时阻断缓存页面在传输过程中非法广告及非法内容、数据的插入
判定原则: 达到以上预期结果,则通过,否则不通过

7.1.1.2 安全审计

第 2 级数据安全审计的测试方法见表 4。

表 4 数据安全审计 2 级测试方法

测试编号:CDN-第 2 级-数据安全-安全审计-01
测试项目:6.1.1.2a)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 180 d,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 180 d;c)保存的操作日志应定期(如每半年/季度/月)进行审计
测试步骤: 1) 查看 CDN 系统日志,判断 CDN 系统是否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; 2) 日志记录是否保存至少 180 d,日志记录是否包含操作人员、操作时间、操作内容,操作结果等信息; 3) 查看 CDN 系统是否记录了 CDN 内部人员管理维护操作和数据访问情况,日志记录是否至少保留了 180 d; 4) 询问 CDN 是否对保存的操作日志定期审计,查看 CDN 是否保留了审计记录
预期结果: 1) 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 180 d,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; 2) 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 180 d; 3) CDN 应对保存的操作日志定期(如每半年/季度/月审核一次)审计
判定原则: 达到以上预期结果,则通过,否则不通过

7.1.1.3 恶意数据清除

第 2 级恶意数据清除的测试方法见表 5。

表 5 恶意数据清除 2 级测试方法

测试编号:CDN-第 2 级-数据安全-恶意数据清除-01
测试项目:6.1.1.3 CDN 系统应根据国家有关部门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 min 内
测试步骤: 1) 通过现网要求 CDN 屏蔽或清除指定页面(模拟被篡改页面或包含恶意代码页面); 2) 验证 CDN 能否根据国家或内容源站要求在约定时间和范围内完成指定页面的屏蔽或清除操作
预期结果: 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 min 内
判定原则: 达到以上预期结果,则通过,否则不通过

7.1.2 业务系统安全

7.1.2.1 结构安全

第2级业务系统结构安全的测试方法见表6。

表6 结构安全2级测试方法

测试编号:CDN-第2级-业务系统安全-结构安全-01
<p>测试项目:6.1.2.1a)CDN系统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系统应做好内外网隔离,内部IPv4地址、IPv6全局地址应拒绝外网直接访问;c)CDN系统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%;d)CDN系统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;e)CDN的中央核心节点(运营管理系统、DNS调度系统、监控系统)有实时备份节点,可在规定时间内切换至备份节点,以保证服务的可持续性;f)CDN系统在单个运营商内至少部署3个节点;g)CDN系统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;h)CDN系统应具有较为完备的IPv4/IPv6安全防护能力,包括安全监测能力、过滤攻击能力、容错能力、负载均衡调度能力,能够防护IPv4/IPv6网络环境下主流的Web应用攻击,例如OWASP排名前十的Web应用程序漏洞等;i)CDN系统应具有抗攻击(如DDoS攻击)和快速恢复能力;j)CDN系统应具备隔离针对单一客户攻击的能力,防止或降低攻击对其他客户的影响</p>
<p>测试步骤:</p> <ol style="list-style-type: none"> 1) 询问CDN运营企业是否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;查看企业的网段划分实际配置,并通过内外网测试验证CDN是否有效限制不同子网或网段之间的访问。 2) 通过现网测试验证CDN内网IPv4地址、IPv6全局地址是否不能从外网直接访问。 3) 通过现网测试验证CDN的节点部署是否能防范安全攻击,抽查现网中单节点(位于独立IDC机房内的CDN服务器群)服务能力(如承载带宽量),与全网服务能力相比判断CDN服务器单节点的服务能力是否不超过全网的20%。 4) 询问CDN是否采用多边缘服务器冗余配置,通过现网检测CDN是否采用多边缘服务器冗余配置抵抗攻击。如抽选一个边缘服务器进行压力测试,确定其冗余配置的边缘服务器,验证该边缘服务器受到攻击并且无法承载时,是否可在规定时间内切换至冗余系统。 5) 查看现网的CDN中央核心节点(运营管理系统、DNS调度系统、监控系统)是否都有实时备份节点,人为构造某个中央核心节点故障,判断是否可以在测试约定时间内切换至备份节点,以保证服务的可持续性。 6) 查看网络配置,验证CDN是否在单个运营商内至少部署3个节点。 7) 询问并查看相关设计文档,判断CDN是否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。 8) 查看现网CDN系统是否有安全监测能力、过滤攻击能力、容错能力、负载均衡调度能力。例如通过压力测试,验证CDN系统是否能产生告警,进而判断其是否具备安全监测能力;通过配置一定的过滤规则,并进行访问测试验证CDN系统是否具备过滤攻击能力;通过对设备人为设置故障,并观察后续的行为来验证是否具备容错能力和负载均衡调度能力。 9) 现网仿真DDoS攻击和黑客入侵攻击,验证CDN系统在运营过程中是否具有抗攻击和快速恢复能力。 10) 询问CDN系统配置的隔离策略,通过仪表对某客户进行压力测试,验证CDN系统在识别出特定客户被攻击时,是否能隔离该客户,以有效防止针对一个客户的攻击影响到其他客户

表 6 结构安全 2 级测试方法（续）

预期结果：
1) CDN 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；
2) CDN 应做好内外网隔离,内部 IPv4 地址、IPv6 全局地址应拒绝外网直接访问；
3) CDN 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%；
4) CDN 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；
5) CDN 的中央核心节点(运营管理系统、DNS 调度系统、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；
6) CDN 在单个运营商内至少部署 3 个节点；
7) CDN 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；
8) CDN 系统应具有较为完备的 IPv4/IPv6 安全防护能力,包括安全监测能力、过滤攻击能力、容错能力、负载均衡调度能力,能够防护 IPv4/IPv6 网络环境下主流的 Web 应用攻击,例如 OWASP TOP 10 的 Web 应用程序漏洞等；
9) CDN 系统应具有抗攻击(如 DDoS 攻击)和快速恢复能力；
10) CDN 系统应能应具备隔离针对单一客户攻击的能力,防止或降低攻击对其他客户的影响
判定原则：
达到以上预期结果,则通过,否则不通过

7.1.2.2 访问控制

第 2 级业务系统访问控制的测试方法见表 7。

表 7 业务系统访问控制 2 级测试方法

测试编号:CDN-第 2 级-业务系统安全-访问控制-01
测试项目:6.1.2.2a)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;d)CDN 内部管理员应从内部网络(或外网 VPN 方式)登录 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 2 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 d);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;h)CDN 系统应具备 IPv4/IPv6 地址的访问控制能力
测试步骤：
1) 现网查看 CDN 系统是否对内部操作维护管理人员进行身份认证；
2) 现网查看 CDN 系统是否对内容源站管理员的登录操作进行身份认证；
3) 现网查看 CDN 系统的身份认证过程是否通过 SSL 通道完成；
4) 询问 CDN 内部管理员是否必须从内部网络(或外网 VPN 方式)登录 CDN 系统,现网测试 CDN 系统是否通过用户密码、登录 IP 地址、黑白名单控制等进行访问限制,是否不存在通过其他方式登录 CDN 系统的情况；
5) 通过仪表测试和现网登录系统验证 CDN 系统的操作维护管理员口令长度是否不小于 8 字节,口令复杂度要求是否足够(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 2 种的组合,且与用户名或 ID 无相关性),口令是否定期更换(更新周期不大于 90 d)；
6) 询问 CDN 系统哪些设备中保存 CDN 系统内部和内容源站操作维护人员信息,现网测试 CDN 系统是否明文保留密码；
7) 现网尝试失败登录,验证 CDN 系统是否采用启用登录失败处理功能,如限制非法登录次数、锁定账号等；
8) 询问 CDN 系统是否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,现网验证上述措施是否落实；
9) 现网查看 CDN 系统是否具备 IPv4/IPv6 地址的访问控制能力

表 7 业务系统访问控制 2 级测试方法 (续)

<p>预期结果:</p> <ol style="list-style-type: none"> 1) CDN 系统应对内部操作维护管理人员进行身份认证; 2) CDN 系统应对内容源站管理员的登录操作进行身份认证; 3) CDN 系统的身份认证过程应通过 SSL 通道完成; 4) CDN 内部管理员应必须从内部网络(或外网 VPN 方式)登录 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; 5) 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 2 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 d); 6) 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; 7) 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; 8) CDN 系统应具备 IPv4/IPv6 地址的访问控制能力
<p>判定原则:</p> <p>达到以上预期结果,则通过,否则不通过</p>

7.1.2.3 攻击防范

第 2 级业务系统攻击防范的测试方法见表 8。

表 8 业务系统攻击防范 2 级测试方法

测试编号:CDN-第 2 级-业务系统安全-攻击防范-01
<p>测试项目:6.1.2.3 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 IPv4/IPv6 网络下的抗攻击/压力保护,包括抗同步泛洪攻击、UDP 泛洪攻击等流量型 DDoS 攻击、承载访问压力等,抗流量型 DDoS 攻击的能力不小于 600 Gbit/s,承载访问压力的能力不小于 3 Gbit/s</p>
<p>测试步骤:</p> <ol style="list-style-type: none"> 1) 通过查看网络拓扑、配置等判断引入 CDN 后是否没有降低内容源站的安全水平; 2) 通过现网仪表压力测试验证 CDN 系统是否能提供对内容源站的抗攻击/压力保护,包括抗同步泛洪攻击、UDP 泛洪攻击等流量型 DDoS 攻击、承载访问压力等
<p>预期结果:</p> <p>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 IPv4/IPv6 网络下的抗攻击/压力保护,包括抗同步泛洪攻击、UDP 泛洪攻击等流量型 DDoS 攻击、承载访问压力等,抗流量型 DDoS 攻击的能力不小于 600 Gbit/s,承载访问压力的能力不小于 3 Gbit/s</p>
<p>判定原则:</p> <p>达到以上预期结果,则通过,否则不通过</p>

7.1.2.4 入侵防范

第 2 级业务系统入侵防范的测试方法见表 9。

表 9 业务系统入侵防范 2 级测试方法

测试编号:CDN-第 2 级-业务系统安全-入侵防范-01
<p>测试项目:6.1.2.4a)CDN 系统应采取安全措施(如 ACL 中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 系统应定期(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入侵</p>
<p>测试步骤:</p> <ol style="list-style-type: none"> 1) 询问 CDN 运营企业采取了哪些防范入侵的安全措施,现网查看是否有效落实了安全措施(如 ACL 中关闭不必要的端口和服务、限制访问地址等)防止 CDN 系统被入侵,测试 CDN 采取了安全措施后是否能够有效防止对 CDN 系统的攻击; 2) 询问并查看记录,判断 CDN 是否定期(每月/季度/半年)对系统进行安全扫描和加固,是否对现网验证安全扫描发现的问题进行了加固

表 9 业务系统入侵防范 2 级测试方法（续）

预期结果： 1) CDN 应采取安全措施(如 ACL 中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； 2) CDN 应定期(每月/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入侵、防篡改、防攻击、防病毒
判定原则： 达到以上预期结果,则通过,否则不通过

7.1.2.5 DNS 调度系统安全

第 2 级业务系统 DNS 调度系统安全的测试方法见表 10。

表 10 DNS 调度系统安全 2 级测试方法

测试编号:CDN-第 2 级-业务系统安全-DNS 调度系统-01
测试项目:6.1.2.5a)CDN 系统的 DNS 调度系统应支持 IPv4/IPv6 协议;b)CDN 系统的 DNS 调度系统应采用最新版本的 DNS 服务器软件;c)CDN 系统的 DNS 调度系统应与所在 CDN 系统具有相同的安全等级,并按照 YD/T 2052—2015 中 5.1~5.3 的安全要求开展与安全等级相应的安全防护工作
测试步骤： 1) 查看 CDN 的现网配置,DNS 权威授权体系是否支持 IPv4/IPv6 协议； 2) 询问 CDN 运营企业对 DNS 服务器软件更新或修补的机制,判断其是否尽可能采用包含最新补丁的 DNS 服务器软件； 3) 询问并查看 CDN 对 DNS 服务器的安全设置,判断其是否对内部所有的 DNS 服务器参照 YD/T 2052—2015 进行了与所在内容分发网络相同级别的安全设置
预期结果： 1) DNS 权威授权体系应支持 IPv4/IPv6 协议； 2) CDN 系统的 DNS 调度系统应采用最新版本的 DNS 服务器软件； 3) CDN 应参照 YD/T 2052—2015 对 DNS 服务器进行与所在内容分发网络相同级别的安全设置
判定原则： 达到以上预期结果,则通过,否则不通过

7.1.2.6 冗余系统、冗余设备及冗余链路要求

第 2 级业务系统冗余系统、冗余设备及冗余链路的测试方法见表 11。

表 11 冗余系统 2 级测试方法

测试编号:CDN-第 2 级-业务系统安全-冗余要求-01
测试项目:6.1.2.6a)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、DNS 调度系统等 CDN 系统的核心系统均应至少有两个备份系统(宜部署在不同省份),保证系统在遇到故障和攻击时应能在 30 min 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(DNS 调度系统、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(DNS 调度系统、运营管理系统、监控系统)间通过多链路相连
测试步骤： 1) 询问并现网查看 CDN 系统是否进行了冗余配置,是否能为多个边缘节点提供安全可靠稳定的服务。询问并查看运营管理系统、DNS 调度系统是否有至少两个备份系统,部署于至少两个省,通过现网测试判断 CDN 系统在遇到故障和内外网攻击时是否能在 30 min 内完成系统切换。 2) 询问 CDN 系统的处理能力是否具备至少 20%的冗余,是否能够满足业务高峰期需要。 3) 访谈查看 CDN 系统的核心系统(DNS 调度系统、运营管理系统、监控系统)链路的连接情况,判断是否有专有链路接入相关运营商,每个核心系统上联接入是否有备份光纤。 4) 访谈查看 CDN 系统的核心系统(DNS 调度系统、运营管理系统、监控系统)间的互联情况,判断是否通过多链路相连

表 11 冗余系统 2 级测试方法（续）

预期结果：
1) 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、DNS 调度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 min 内完成系统切换；
2) 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；
3) CDN 系统的核心系统(DNS 调度系统、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；
4) CDN 系统的核心系统(DNS 调度系统、运营管理系统、监控系统)间通过多链路相连
判定原则：
达到以上预期结果,则通过,否则不通过

7.1.3 主机安全

7.1.3.1 访问控制

第 2 级主机安全访问控制的测试方法见表 12。

表 12 主机安全访问控制 2 级测试方法

测试编号:CDN-第 2 级-主机安全-访问控制-01
测试项目:6.1.3.1a)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 8 位,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 2 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 d);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 系统应及时删除多余的、过期的账户,避免共享账户的存在;h)CDN 系统应实现操作系统和数据库系统特权用户的权限分离;i)CDN 系统应限制默认账户的访问权限,修改这些账户的默认口令,设备功能配置可更改的情况下,应重命名默认账户;j)CDN 系统应能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力,控制粒度到主机级
测试步骤：
1) 通过现网测试验证系统是否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；
2) 通过现网测试验证系统是否对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；
3) 通过现网测试验证系统操作系统和数据库系统管理用户身份标识具有不易被冒用的特点,相关用户口令长度不小于 8 位,口令有复杂度要求(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 2 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 d)；
4) 通过现网尝试失败的登录,测试 CDN 系统是否启用登录失败处理功能,如采取结束会话、限制非法登录次数和自动退出等措施；
5) 询问并现网验证当对各类 CDN 主机进行远程管理时,CDN 系统是否采取必要措施(如使用加密协议)防止鉴别信息在传输过程中被窃听；
6) 询问并现网测试验证 CDN 系统是否启用了访问控制机制或策略,是否可以依据安全策略控制操作维护人员对资源的访问；
7) 询问并现网验证 CDN 是否及时删除系统多余的、过期的账户,避免共享账户的存在；
8) 询问 CDN 系统中操作系统和数据库系统特权用户的关系,现网验证 CDN 是否实现操作系统和数据库系统特权用户的权限分离；
9) 询问 CDN 系统的账户管理机制,现网验证 CDN 是否限制默认账户的访问权限,修改这些账户的默认口令,设备功能配置可更改情况下是否重命名默认账户

表 12 主机安全访问控制 2 级测试方法（续）

预期结果：
1) 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；
2) 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；
3) 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 8 位，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 2 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 d）；
4) 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；
5) 当对各类主机进行远程管理时，CDN 系统应采取措施（如使用加密协议）防止鉴别信息在传输过程中被窃听；
6) 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；
7) CDN 应及时删除多余的、过期的账户，避免共享账户的存在；
8) CDN 应实现操作系统和数据库系统特权用户的权限分离；
9) CDN 应限制默认账户的访问权限，修改这些账户的默认口令，设备功能配置可更改的情况下，应重命名默认账户
判定原则：
达到以上预期结果，则通过，否则不通过

7.1.3.2 安全审计

第 2 级主机安全审计的测试方法见表 13。

表 13 主机安全审计 2 级测试方法

测试编号：CDN-第 2 级-主机安全-安全审计-01
测试项目：6.1.3.2a) 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 系统应保护审计记录，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 d）
测试步骤：
1) 查看审计记录，判断 CDN 的审计范围是否覆盖到主机/服务器上的每个操作系统用户和数据库用户；
2) 查看审计记录，判断 CDN 的审计内容是否包括重要用户行为、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；
3) 查看审计记录，判断审计记录是否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；
4) 询问 CDN 有哪些保护审计记录，以避免其受到未预期的删除、修改或覆盖等的措施，判断这些措施是否能有效落实，审计记录是否能保留至少 180 d
预期结果：
1) 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；
2) 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；
3) 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；
4) CDN 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 d）
判定原则：
达到以上预期结果，则通过，否则不通过

7.1.3.3 入侵防范

第 2 级主机安全入侵防范的测试方法见表 14。

表 14 主机安全入侵防范 2 级测试方法

测试编号:CDN-第 2 级-主机安全-入侵防范-01
测试项目:6.1.3.3 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。主机和网络层面均应部署防入侵、防病毒软件或者硬件
测试步骤: 1) 询问 CDN 运营企业的操作系统安全原则,判断操作系统是否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; 2) 询问和查验 CDN 系统是否部署防入侵、防病毒软件或者硬件
预期结果: 1) 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; 2) 主机和网络层面均应部署防入侵、防病毒软件或者硬件
判定原则: 达到以上预期结果,则通过,否则不通过

7.1.3.4 资源控制

第 2 级主机安全资源控制的测试方法见表 15。

表 15 主机安全资源控制 2 级测试方法

测试编号:CDN-第 2 级-主机安全-资源控制-01
测试项目:6.1.3.4a)CDN 系统应对边缘服务器、核心系统(DNS 调度系统、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 系统应能够对服务器、数据库等系统的服务水平设定告警阈值,当监测到服务水平指标触发阈值时应能进行告警
测试步骤: 1) 现网查看监控记录,判断 CDN 系统是否对边缘服务器、核心系统(DNS 调度系统、运营管理系统、监控系统)进行监测,包括监测服务器的 CPU、硬盘、内存、网络等资源的使用情况; 2) 现网查看监控记录,判断 CDN 系统是否对所有的服务器、数据库的服务水平设定告警阈值
预期结果: 1) CDN 应对边缘服务器、核心系统(DNS 调度系统、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; 2) CDN 应能够对服务器、数据库等系统的服务水平设定告警阈值,当监测到服务水平指标触发阈值时应能进行告警
判定原则: 达到以上预期结果,则通过,否则不通过

7.1.4 物理环境安全

第 2 级物理环境安全的测试方法见表 16。

表 16 物理环境安全 2 级测试方法

测试编号: CDN-第 2 级-物理环境安全-01
测试项目: 6.1.4 应满足 GB/T 22239—2019 中第二级的安全物理环境要求
测试步骤: 1) 访谈物理环境管理人员, 查看物理环境设计文档、管理制度、维护记录等, 查看其是否符合 GB/T 22239—2019 中第二级的相关要求; 2) 现场检查 CDN 所处的物理环境
预期结果: CDN 物理环境的安全要求符合 GB/T 22239—2019 中第二级的相关要求
判定原则: 达到以上预期结果, 则通过, 否则不通过

7.1.5 管理安全

第 2 级管理安全的测试方法见表 17。



表 17 管理安全 2 级测试方法

测试编号: CDN-第 2 级-管理安全-01
测试项目: 6.1.5 除满足 GB/T 22239—2019 中第二级的安全管理制度、安全管理机构、安全管理人员、安全运维管理相关要求外, 还应满足以下要求: a) 监控人员应能够及时发现安全攻击和系统宕机等异常事件, 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; b) 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; c) 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; d) CDN 系统应针对各类安全攻击(如 CDN 遭受 DDoS 攻击, DNS 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; e) CDN 系统应对 CDN 全网系统有 7×24 h 监控; f) CDN 系统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); g) CDN 系统应对灾难恢复预案进行教育、培训和演练
测试步骤: 1) 访谈网络安全管理人员, 查看与网络安全管理相关的资料等, 查看其是否符合 GB/T 22239—2019 中第二级的相关要求; 2) 询问 CDN 运营企业的监控项目与相关安全预案, 验证 CDN 企业的监控人员是否能够及时发现安全攻击和系统宕机等异常事件, 并在企业事先规定时间内汇报运维人员、管理人员和公司核心管理人员, 同时在事先规定时间内通知内部客户服务人员; 3) 查看 CDN 的安全预案, 现网验证运维人员是否能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; 4) 查看 CDN 的相关管理流程, 现网验证客服人员是否能及时(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; 5) 现网验证 CDN 是否能针对各类安全攻击(如 CDN 遭受 DDoS 攻击, DNS 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; 6) 询问并现网验证 CDN 是否对 CDN 全网系统有 7×24 h 监控; 7) 询问并现网验证 CDN 的针对灾难的服务恢复时间是否能满足企业要求(按照服务协议条款); 8) 询问并查看相关记录, 判断 CDN 是否对灾难恢复预案进行过教育、培训和演练, 这些教育、培训和演练是否能够有效提高 CDN 的安全能力

表 17 管理安全 2 级测试方法（续）

预期结果： 1) 管理安全要求符合 GB/T 22239—2019 中第二级的相关要求； 2) 监控人员应能够及时发现安全攻击和系统宕机等异常事件，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； 3) 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； 4) 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； 5) CDN 应针对各类安全攻击（如 CDN 遭受 DDoS 攻击，DNS 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； 6) CDN 应对 CDN 全网系统有 7×24 h 监控； 7) CDN 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）； 8) CDN 应对灾难恢复预案进行教育、培训和演练
判定原则： 达到以上预期结果，则通过，否则不通过

7.2 第 3 级测试方法



7.2.1 数据安全

7.2.1.1 数据一致性保护

第 3 级数据一致性保护除按照 7.1.1.1 的测试方法进行测试之外，还应按照表 18 的要求进行测试。

表 18 数据一致性保护 3 级测试方法

测试编号：CDN-第 3 级-数据安全-数据一致性保护-01
测试项目：6.2.1.1a)CDN 系统应有能力保证 CDN 数据与内容源站传输的一致性，支持 MD5 值比对、Etag 值比对等方式保证 CDN 数据与内容源站传输的一致性；b)CDN 系统应具有防止 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
测试步骤： 1) 询问并测试验证 CDN 是否有能力保证 CDN 数据与内容源站传输数据一致性，查验是否通过 MD5 值比对、Etag 值比对等方式保证 CDN 数据与内容源站传输的一致性； 2) 测试者提供一个源站，被测试者提供缓存服务器，测试者向缓存服务器请求测试的 URL，在传输过程中测试者篡改源站与缓存服务器之间传输的数据，测试者应无法获得被篡改的数据； 3) 清除缓存，测试者再次向缓存服务器请求同样的 URL，不执行篡改操作，测试者得到结果后与源站内容对比，预期结果应完全一致； 4) 询问 CDN 运营企业是否具有防止 CDN 边缘服务器回源站域名解析遭到劫持的能力和措施，现网测试验证在源站配合下，CDN 的边缘服务器是否能避免受到公网 DNS 的污染或者劫持进而向错误的源站发出内容请求
预期结果： 1) CDN 应有能力保证 CDN 数据与内容源站传输的一致性，支持 MD5 值比对、Etag 值比对等方式保证 CDN 数据与内容源站传输的一致性； 2) CDN 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
判定原则： 达到以上预期结果，则通过，否则不通过

7.2.1.2 安全审计

第 3 级数据安全审计除按照 7.1.1.2 的测试方法进行测试之外,还应按照表 19 的要求进行测试。

表 19 数据安全审计 3 级测试方法

测试编号:CDN-第 3 级-数据安全-安全审计-01
测试项目:6.2.1.2 应具有对审计记录数据进行统计、查询、分析及生成审计报表的功能
测试步骤: 查看 CDN 是否保留了审计记录,是否有对审计记录数据进行统计、查询、分析及生成审计报表的功能
预期结果: 应具有对审计记录数据进行统计、查询、分析及生成审计报表的功能
判定原则: 达到以上预期结果,则通过,否则不通过

7.2.1.3 恶意数据清除

第 3 级恶意数据清除除按照 7.1.1.3 的测试方法进行测试之外,还应按照表 20 的要求进行测试。

表 20 恶意数据清除 3 级测试方法

测试编号:CDN-第 3 级-数据安全-恶意数据清除-01
测试项目:6.2.1.3 CDN 系统应能够在国家相关部门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 10 min 内
测试步骤: 通过现网要求 CDN 屏蔽或清除指定页面(模拟被篡改页面或包含恶意代码页面),验证 CDN 能否根据国家或内容源站要求在约定时间和范围内完成指定页面的屏蔽或清除操作
预期结果: 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 10 min 内
判定原则: 达到以上预期结果,则通过,否则不通过

7.2.1.4 备份数据安全

备份数据安全的测试方法见表 21。

表 21 备份数据安全测试方法

测试编号:CDN-第 3 级-数据安全-备份数据安全-01
测试项目:6.2.1.4a)CDN 系统应在多个核心节点备份运营管理系统的系统管理数据,应每 10 min 同步一次;b)CDN 系统应对源站托管数据进行多点容灾备份,应在 10 min 内完成数据同步
测试步骤: 1) 询问 CDN 运营企业在哪些核心节点备份运营管理系统的系统管理数据,查看同步一次的时间间隔是否不大于 10 min; 2) 询问 CDN 运营企业是否对源站托管数据进行多点容灾备份,在哪些地方进行了容灾备份,查看是否能在 10 min 完成数据同步

表 21 备份数据安全测试方法（续）

预期结果： 1) CDN 应在多个核心节点备份运营管理系统系统管理数据，应每 10 min 同步一次； 2) CDN 应对源站托管数据进行多点容灾备份，应在 10 min 完成数据同步
判定原则： 达到以上预期结果，则通过，否则不通过

7.2.2 业务系统安全

7.2.2.1 结构安全

第 3 级业务系统结构安全按照 7.1.2.1 的测试方法进行测试之外，还应按照表 22 的要求进行测试。

表 22 业务系统结构安全 3 级测试方法

测试编号:CDN-第 3 级-业务系统安全-结构安全-01
测试项目:6.2.2.1 CDN 系统在单个运营商内至少部署 10 个节点
测试步骤： 询问 CDN 运营企业在哪些运营商部署了节点，是否在单个运营商内至少部署 10 个节点
预期结果： CDN 在单个运营商内至少部署 10 个节点
判定原则： 达到以上预期结果，则通过，否则不通过

7.2.2.2 访问控制

第 3 级业务系统访问控制按照 7.1.2.2 的测试方法进行测试之外，还应按照表 23 的要求进行测试。

表 23 业务系统访问控制 3 级测试方法

测试编号:CDN-第 3 级-业务系统安全-访问控制-01
测试项目:6.2.2.2 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
测试步骤： 现网查看 CDN 系统是否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，验证访问权限限制是否有效
预期结果： 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
判定原则： 达到以上预期结果，则通过，否则不通过

7.2.2.3 攻击防范

第 3 级业务系统攻击防范按照 7.1.2.3 的测试方法进行测试之外，还应按照表 24 的要求进行测试。

表 24 业务系统攻击防范 3 级测试方法

测试编号:CDN-第 3 级-业务系统安全-攻击防范-01
测试项目:6.2.2.3a)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 IPv4/IPv6 网络下的抗攻击/压力保护,包括抗同步泛洪攻击、UDP 泛洪攻击等流量型 DDoS 攻击,承载访问压力等,抗流量型 DDoS 攻击的能力不小于 1.2 Tbit/s,承载访问压力的能力不小于 10 Gbit/s;b)当攻击量或访问压力超过 CDN 的承载能力,CDN 系统应能够采取有效措施避免造成 CDN 网络的全面瘫痪
测试步骤: 1) 通过查看网络拓扑、配置等判断引入 CDN 后是否没有降低内容源站的安全水平。通过现网仪表压力测试验证 CDN 系统是否能提供对内容源站 IPv4/IPv6 网络下的抗攻击/压力保护,包括抗同步泛洪攻击、UDP 泛洪攻击等流量型 DDoS 攻击,承载访问压力等。具体指标建议抗流量型 DDoS 攻击的能力不小于 1.2 Tbit/s,承载访问压力 10 Gbit/s。 2) 通过访谈和查看配置判断当攻击量或访问压力超过 CDN 的承载能力,CDN 是否能够采取有效措施避免造成 CDN 网络的全面瘫痪
预期结果: 1) 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 IPv4/IPv6 网络下的抗攻击/压力保护,包括抗同步泛洪攻击、UDP 泛洪攻击等流量型 DDoS 攻击,承载访问压力等,抗流量型 DDoS 攻击的能力不小于 1.2 Tbit/s,承载访问压力的能力不小于 10 Gbit/s; 2) 当攻击量或访问压力超过 CDN 的承载能力,CDN 应能够采取有效措施避免造成 CDN 网络的全面瘫痪
判定原则: 达到以上预期结果,则通过,否则不通过

7.2.2.4 入侵防范

同 7.1.2.4 测试方法。

7.2.2.5 DNS 调度系统安全

第 3 级 DNS 调度系统安全按照 7.1.2.5 的测试方法进行测试之外,还应按照表 25 的要求进行测试。

表 25 DNS 调度系统安全 3 级测试方法

测试编号:CDN-第 3 级-业务系统安全-DNS 调度系统安全-01
测试项目:6.2.2.5a)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 96 h 内历史访问量采样集的 3 倍访问量;c)CDN 的 DNS 服务应根据国家相关要求在相应部门注册
测试步骤: 1) 现网仿真攻击 DNS 验证 CDN 的 DNS 服务解析是否具有抗攻击能力,CDN 系统是否支持 DNS 系统监控、DNS 可用性(外部可访问)监控、DNS 防攻击等; 2) 询问并查看 DNS 配置,判断 DNS 是否可处理整个系统的 96 h 内历史访问量采样集的 3 倍访问量; 3) 询问 CDN 运营企业部署了哪些 DNS 服务器节点进行冗余备份,判断其在全国是否至少部署三个 DNS 系统节点进行冗余备份; 4) 询问 CDN 的 DNS 服务在哪些部门进行了注册,查看相关注册信息

表 25 DNS 调度系统安全 3 级测试方法（续）

预期结果： 1) 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； 2) DNS 可处理整个系统的 96 h 内历史访问量采样集的 3 倍访问量； 3) 全国至少部署三个 DNS 系统节点进行冗余备份； 4) CDN 的 DNS 服务应根据国家相关要求在相应部门注册
判定原则： 达到以上预期结果，则通过，否则不通过

7.2.2.6 冗余系统、冗余设备及冗余链路

第 3 级冗余系统、冗余设备和冗余链路按照 7.1.2.6 的测试方法进行测试之外，还应按照表 26 的要求进行测试。

表 26 冗余系统 3 级测试方法

测试编号：CDN-第 3 级-业务系统安全-冗余要求-01
测试项目：6.2.2.6 CDN 系统的 DNS 调度系统、配置管理系统应有多份（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
测试步骤： 询问并查看 CDN 系统的 DNS 系统是否有多份（至少四份）备份系统，测试 CDN 系统的 DNS 系统在遇到故障和攻击时是否能无缝完成系统切换
预期结果： CDN 系统的 DNS 系统、配置管理系统应有多份（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
判定原则： 达到以上预期结果，则通过，否则不通过

7.2.3 主机安全

同 7.1.3 测试方法。

7.2.4 物理环境安全

第 3 级物理环境安全的测试方法见表 27。

表 27 物理环境安全 3 级测试方法

测试编号：CDN-第 3 级-物理环境安全-01
测试项目：6.2.4 应满足 GB/T 22239—2019 中第三级的安全物理环境要求
测试步骤： 1) 访谈物理环境管理人员，查看物理环境设计文档、管理制度、维护记录等，查看其是否符合 GB/T 22239—2019 中第三级的相关要求； 2) 现场检查 CDN 所处的物理环境
预期结果： CDN 物理环境的安全要求符合 GB/T 22239—2019 中第三级的相关要求
判定原则： 达到以上预期结果，则通过，否则不通过

7.2.5 管理安全

第 3 级管理安全按照 7.1.5 的测试方法进行测试之外,还应按照表 28 的要求进行测试。

表 28 管理安全 3 级测试方法

测试编号:CDN-第 3 级-管理安全-01
测试项目:6.2.5 应满足第 2 级以及 GB/T 22239—2019 中第三级的安全管理制度、安全管理机构、安全管理人员、安全运维管理相关要求
测试步骤: 访谈网络安全管理人员,查看与网络安全管理相关的资料等,查看其是否符合 GB/T 22239—2019 中第三级的相关要求
预期结果: 管理安全要求符合 GB/T 22239—2019 中第三级的相关要求
判定原则: 达到以上预期结果,则通过,否则不通过



参 考 文 献

- [1] 关于加快推进互联网协议第六版(IPv6)规模部署和应用工作的通知(中网办发文〔2021〕15号)
-

