

YDB

中国通信标准化协会标准

YDB 115—2012

互联网内容分发网络安全防护检测要求

Security Protection Test 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	II
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	1
4 互联网内容分发网络安全防护检测概述	2
4.1 互联网内容分发网络安全防护检测范围	2
4.2 互联网内容分发网络安全防护检测对象	2
5 互联网内容分发网络安全防护检测要求	2
5.1 第1级要求	2
5.2 第2级要求	2
5.2.1 数据安全	2
5.2.2 业务系统安全	3
5.2.3 基础设施安全	5
5.2.4 管理安全	6
5.3 第3.1级要求	7
5.3.1 数据安全	7
5.3.2 业务系统安全	7
5.3.3 基础设施安全	8
5.3.4 管理安全	8
5.4 第3.2级要求	8
5.4.1 数据安全	8
5.4.2 业务系统安全	9
5.4.3 基础设施安全	10
5.4.4 管理安全	10
5.5 第4级要求	10
5.6 第5级要求	10

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防护检测要求》；
- 32、《电信网和互联网管理安全检测要求》；
- 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 114-2012《互联网内容分发网络安全防护要求》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、北京蓝汛通信技术有限公司、网宿科技股份有限公司、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。

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检测要求

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检测要求。
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。

GB/T 5271.8-2001	信息技术 词汇 第8部分：安全
YDB 114-2012	互联网内容分发网络安全防护要求
YD/T 1755-2008	电信网和互联网物理环境安全等级保护检测要求
YD/T 1757-2008	电信网和互联网管理安全等级保护检测要求

3 术语、定义和缩略语

3.1 术语和定义

GB/T 5271.8-2001确立的术语和定义，以及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。重要程度从信息服务系统受到破坏后，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失来衡量。

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检测 security testing of CDN

对互联网内容分发网络的安全保护能力是否达到相应安全等级的安全防护要求进行衡量。

3.1.4

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检测概述

4.1 互联网内容分发网络安全防护检测范围

本标准的安全防护检测范围与YDB 114-2012《互联网内容分发网络安全防护要求》一致。

4.2 互联网内容分发网络安全防护检测对象

互联网内容分发网络的安全防护检测对象是作为第三方对外提供互联网内容分发服务的网络或系统，本标准主要对互联网内容分发网络的各项要求的实施进行检测。

5 互联网内容分发网络安全防护检测要求

5.1 第1级要求

不作要求。

5.2 第2级要求

5.2.1 数据安全

5.2.1.1 数据一致性保护

数据一致性保护要求如下：

- a) 询问并测试验证 CDN 运营企业是否有能力保证 CDN 平台内部传输数据一致性。例如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；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，预期结果应完全一致；
- b) 询问 CDN 运营企业是否有能力保护分发的内容不被非法引用，现网测试验证 CDN 系统是否有能力支持基于访问 IP、访问来源、时间等方式的防盗链。例如 CDN 运营企业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，如果无法访问即判定为基于访问来源的防盗链措施有效；CDN 运营企业对链接进行访问 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，访问失败，测试人员通过在 IP 范围内的 IP 地址访问，访问成功即判定为基于 IP 的防盗链措施有效；CDN 运营企业进行访问时间防盗链配置，测试人员在配置时间外访问失败，在配置时间内访问成功，即可判定系统支持基于时间的防盗链。

5.2.1.2 安全审计

安全审计要求如下：

- a) 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, 日志记录是否保存至少 60 天, 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;
- b) 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 90 天;
- c) 询问 CDN 运营企业是否对保存的操作日志定期审计 (如每半年/季度/月审核一次), 查看 CDN 运营企业是否保留了审计记录。

5.2.1.3 恶意数据清除

通过现网要求 CDN 运营企业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 运营企业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, 保证全网服务器屏蔽或清除全部指定页面的系统完成时间在 30 分钟内。

5.2.2 业务系统安全

5.2.2.1 结构安全

结构安全要求如下:

- a) 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 运营企业是否有效限制不同子网或网段之间的访问;
- b) 通过现网测试验证 CDN 运营企业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%;
- c) 询问 CDN 运营企业是否采用多边缘服务器冗余配置, 通过现网检测 CDN 运营企业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;
- d) 查看现网的 CDN 中央核心节点 (运营管理系统、请求路由系统、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;
- e) 查看网络配置, 验证 CDN 运营企业是否在单个运营商内至少部署 3 个节点;
- f) 询问并查看相关设计文档, 判断 CDN 运营企业是否在软件结构上将各功能模块化, 从而实现软件精细化管理, 一个软件的故障不影响其他软件提供服务;
- g) 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;
- h) 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;
- i) 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。

5.2.2.2 访问控制

访问控制要求如下:

- a) 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；
- b) 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；
- c) 现网查看 CDN 系统的身份认证过程是否通过 SSL 通道完成；
- d) 询问 CDN 内部管理员是否必须从公司内部（包含外网 VPN 方式）登陆 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；
- e) 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二种的组合，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 天）；
- f) 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；
- g) 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；
- h) 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。

5.2.2.3 用户信息保护

用户信息保护要求如下：

- a) 询问并现场查验 CDN 系统是否对 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，是否采取有效措施防止用户信息被泄露、滥用；
- b) 询问并现场查验未经内容源站允许，CDN 运营企业是否未截获、存储互联网用户访问中的个人信息；
- c) 询问并现场查验 CDN 系统是否加密保留 CDN 系统内部和内容源站操作维护人员的访问密码。

5.2.2.4 攻击防范

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。

5.2.2.5 入侵防范

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有效防止对 CDN 系统的攻击。

询问并查看记录，判断 CDN 运营企业是否定期（每个月/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。

5.2.2.6 请求路由系统安全

请求路由系统安全要求如下：

- a) 查看 CDN 运营企业的现网配置，验证其在全国是否至少部署两个 DNS 节点进行冗余备份；
- b) 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；

- c) 询问并查看 CDN 运营企业对 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《域名系统安全防护要求》进行了与所在互联网内容分发网络相同级别的安全设置。

5.2.2.7 冗余系统、冗余设备及冗余链路要求

冗余系统、冗余设备及冗余链路要求如下:

- a) 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、请求路由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 分钟内完成系统切换;
- b) 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;
- c) 询问 CDN 运营企业 CDN 系统的核心系统(请求路由系统、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;
- d) 询问 CDN 运营企业 CDN 系统的核心系统(请求路由系统、运营管理系统、监控系统)间的互联情况,判断是否通过多链路相连。

5.2.3 基础设施安全

5.2.3.1 主机安全

5.2.3.1.1 访问控制

访问控制要求如下:

- a) 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;
- b) 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;
- c) 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 6 字节,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) 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;
- e) 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;
- f) 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;
- g) 询问并现网验证 CDN 运营企业是否及时删除系统多余的、过期的帐户,避免共享帐户的存在;
- h) 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 运营企业是否实现操作系统和数据库系统特权用户的权限分离;
- i) 询问 CDN 系统的账户管理机制,现网验证 CDN 运营企业是否限制默认帐户的访问权限,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。

5.2.3.1.2 安全审计

安全审计要求如下:

- a) 查看审计记录,判断 CDN 运营企业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;

- b) 查看审计记录,判断 CDN 运营企业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;
- c) 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;
- d) 询问 CDN 运营企业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够有效落实,审计记录是否能保留至少 180 天。

5.2.3.1.3 入侵防范

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。

5.2.3.1.4 资源控制

资源控制要求如下:

- a) 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(请求路由系统、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;
- b) 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,当监测到服务水平降低到阈值时应能进行告警。

5.2.3.2 物理环境安全

应按照 YD/T 1755-2008 第 2 级要求进行检测。

5.2.4 管理安全

应按照 YD/T 1757-2008 第 2 级要求进行检测。此外,还应按照如下要求进行检测:

- a) 询问 CDN 运营企业是否要求员工需经过培训并通过考核才能上岗,查看培训和考核记录判断要求是否落实;
- b) 询问 CDN 运营企业是否为内容源站提供 7X24 技术支持;
- c) 询问 CDN 运营企业是否有专职的安全管理责任人;
- d) 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当机等异常事件,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;
- e) 查看 CDN 运营企业的安全预案,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;
- f) 查看 CDN 运营企业的相关管理流程,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;
- g) 现网验证 CDN 运营企业是否能针对各类安全攻击(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) 询问并现网验证 CDN 运营企业是否对 CDN 全网系统有 7X24 小时监控;
- i) 询问并现网验证 CDN 运营企业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);
- j) 询问并查看相关记录,判断 CDN 运营企业是否对灾难恢复预案进行过教育、培训和演练,这些教育、培训和演练是否能有效提高 CDN 运营企业的安全能力。

5.3 第3.1级要求

5.3.1 数据安全

5.3.1.1 数据一致性保护

在按照第2级要求检测基础上，还应询问并测试验证CDN运营企业是否有能力保证CDN数据与内容源站传输数据一致性。例如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；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。

5.3.1.2 安全审计

同第2级的检测要求。

5.3.1.3 恶意数据清除

在按照第2级要求检测基础上，还应通过现网要求CDN运营企业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运营企业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，保证全网服务器屏蔽或清除全部指定页面的系统完成时间在15分钟内。

5.3.1.4 版权保护

在按照第2级要求检测基础上，还应检测如下内容：

- 询问CDN运营企业与哪些内容源站商定了具体的版权保护措施和方法，共同实现版权保护。查看相关文档并现网测试验证CDN系统是否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；
- 询问CDN运营企业采用了哪些公开技术保护版权，是否支持公开版权保护技术；
- 询问CDN运营企业是否支持客户定制的内容保护技术和内容解密途径；
- 询问CDN系统是否支持基于用户身份验证（包括回源站认证以及CDN代验证）的版权保护；
- 现网查看并测试CDN系统是否支持基于用户访问的时间特性进行认证；
- 现网查看并测试CDN系统是否支持基于用户使用的IP地址进行访问限制。

5.3.1.5 备份数据安全

在按照第2级要求检测基础上，还应检测如下内容：

- 询问CDN运营企业在哪些核心节点备份配置管理系统的系统管理数据，判断CDN运营企业是否在多个核心节点备份系统管理数据，同步一次的时间间隔是否不大于30分钟；
- 询问CDN运营企业是否对源站托管数据进行多点容灾备份，是否能在30分钟完成数据同步。

5.3.2 业务系统安全

5.3.2.1 结构安全

在按照第2级要求检测基础上，还应询问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。

5.3.2.2 访问控制

同第2级检测要求。

5.3.2.3 用户信息保护

同第2级检测要求。

5.3.2.4 攻击防范

在按照第2级要求检测基础上，还应检测如下内容：

- a) 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的抗攻击/压力保护，包括抗 Synflood、UDPFlood、ACKFlood 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 2Gbps，承载访问压力 10Gbps；
- b) 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 运营企业是否能够采取有效措施避免造成 CDN 网络的全面瘫痪。

5.3.2.5 入侵防范

同3.1级检测要求。

5.3.2.6 请求路由系统安全

在按照第2级要求检测基础上，还应检测如下内容：

- a) 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；
- b) 询问并查看 DNS 配置，判断 DNS 是否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) 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请求路由系统节点进行冗余备份。

5.3.2.7 冗余系统、冗余设备及冗余链路

同第2级检测要求。

5.3.3 基础设施安全

同第2级检测要求。

5.3.4 管理安全

应满足第2级、YD/T 1757-2008中第3.1级的相关检测要求。

5.4 第3.2级要求

5.4.1 数据安全

5.4.1.1 数据一致性保护

在按照第3.1级要求检测基础上，还应询问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。

5.4.1.2 安全审计

同3.1级检测要求。

5.4.1.3 恶意数据清除

在按照第3.1级要求检测基础上,还应通过现网要求CDN运营企业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运营企业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,保证全网服务器屏蔽或清除全部指定页面的系统完成时间在10分钟内。

5.4.1.4 版权保护

在按照第3.1级要求检测基础上,还应询问并查看CDN运营企业是否对不同类型终端(机顶盒、手机、PC等)均提供版权保护,验证这些措施是否有效。

5.4.1.5 备份数据安全

在按照第3.1级要求检测基础上,还应检测如下内容:

- a) 询问CDN运营企业在哪些核心节点备份运营管理系统的数据,查看同步一次的时间间隔是否不大于10分钟;
- b) 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分钟完成数据同步。

5.4.2 业务系统安全

5.4.2.1 结构安全

同3.1级检测要求。

5.4.2.2 访问控制

在按照第3.1级要求检测基础上,还应检测现网查看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。

5.4.2.3 用户信息保护

同第3.1级检测要求。

5.4.2.4 攻击防范

同第3.1级检测要求。

5.4.2.5 入侵防范

同第3.1级检测要求。

5.4.2.6 请求路由系统安全

在按照第3.1级要求检测基础上,还应询问CDN的DNS服务在哪些部门进行了注册,查看相关注册信息,判断CDN运营企业是否有机制和制度根据国家要求完成紧急事件处理。

5.4.2.7 冗余系统、冗余设备及冗余链路要求

在按照第3.1级要求检测基础上,还应询问并查看CDN系统的请求路由系统是否有多份(至少四份)备份系统,测试CDN系统的请求路由系统在遇到故障和攻击时是否能无缝完成系统切换。

5.4.3 基础设施安全

同第3.1级检测要求。

5.4.4 管理安全

在按照第3.1级、YD/T 1757-2008要求检测基础上，还应检测如下内容：

- a) 查看培训和考核记录，检查 CDN 运营企业是否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) 查看教育、培训和演练记录，检查 CDN 运营企业是否定期（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。

5.5 第4级要求

同3.2级检测要求。

5.6 第5级要求

待补充。

YDB 115-2012

中国通信标准化协会标准
互联网内容分发网络安全防护检测要求
YDB 115-2012

*

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