

ICS 33.040.20
M 33



中华人民共和国通信行业标准

YD/T 2242-2011

WAP网关系统安全防护检测要求

Security protection testing requirements for WAP gateway system

2011-06-01 发布

2011-06-01 实施

中华人民共和国工业和信息化部 发布

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.....3

4 WAP 网关系统安全防护检测概述.....3

 4.1 安全防护检测范围.....3

 4.2 安全防护检测对象.....3

 4.3 安全防护检测内容.....4

 4.4 安全防护检测结果判定.....4

5 WAP 网关系统安全等级保护检测要求.....5

 5.1 第1级检测要求.....5

 5.2 第2级检测要求.....5

 5.3 第3.1级检测要求.....7

 5.4 第3.2级检测要求.....10

 5.5 第4级检测要求.....10

 5.6 第5级检测要求.....10

6 WAP 网关系统安全风险评估检测要求.....10

 6.1 安全风险评估范围.....10

 6.2 安全风险评估内容.....11

 6.3 安全风险评估要素.....11

 6.4 安全风险评估赋值原则.....12

 6.5 安全风险评估计算方法.....13

 6.6 安全风险评估文件类型.....13

 6.7 安全风险评估文件记录.....14

7 WAP 网关系统灾难备份及恢复检测要求.....14

 7.1 第1级检测要求.....14

 7.2 第2级检测要求.....14

 7.3 第3.1级检测要求.....16

 7.4 第3.2级检测要求.....18

 7.5 第4级检测要求.....18

 7.6 第5级检测要求.....18

参考文献.....19

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. 《移动通信网系统安全防护要求》
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. 《移动通信系统安全防护检测要求》
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》

本标准与YD/T 2241-2011《WAP网关系统安全防护要求》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。

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。

本标准主要起草人：崔媛媛、袁 琦。

WAP网关系统安全防护检测要求

1 范围

本标准规定了WAP网关系统在风险评估、安全等级保护、灾难备份及恢复等方面的安全防护检测要求。

本标准适用于公众电信网中的WAP网关系统的安全防护检测。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准。然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

YD 5098-2005	《通信局（站）防雷与接地工程设计规范》
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
	移动上网日志留存规范

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

WAP网关系统安全等级 Security Classification of Mobile Communication Network

WAP网关系统安全重要程度的表征。重要程度可从WAP网关系统受到破坏后，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害来衡量。

3.1.2

WAP网关系统安全等级保护 Classified Security Protection of Mobile Communication Network
对WAP网关系统分等级实施安全保护。

3.1.3

组织 Organization

组织是由WAP网关系统中不同作用的个体为实施共同的业务目标而建立的结构，组织的特性在于为完成目标而分工、合作；一个单位是一个组织，某个业务部门也可以是一个组织。

3.1.4

WAP网关系统安全风险 Security Risk of Mobile Communication Network

人为或自然的威胁利用WAP网关系统及其管理体系中存在的脆弱性导致安全事件的发生及其对组织造成的影响。

3.1.5

WAP网关系统安全风险评估 Security Risk Assessment of Mobile Communication Network

指运用科学的方法和手段，系统地分析WAP网关系统所面临的威胁及其存在的脆弱性，评估安全事件一旦发生可能造成的危害程度。为进一步提出有针对性的抵御威胁的防护对策和安全措施，防范和化解WAP网关系统安全风险，将风险控制在可接受的水平，最大限度地保障WAP网关系统的安全提供科学依据。

3.1.6

WAP网关系统资产 Asset of Mobile Communication Network

WAP网关系统中具有价值的资源，是安全防护保护的对象。WAP网关系统中的资产可能是以多种形式存在，无形的、有形的、硬件、软件，包括WAP网关、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WAP网关系统节点设备、WAP网关系统的链路、WAP网关系统的网络布局等。

3.1.7

WAP网关系统资产价值 Asset Value of Mobile Communication Network

WAP网关系统中资产的重要程度或敏感程度。资产价值是资产的属性，也是进行资产识别的主要内容。

3.1.8

WAP网关系统威胁 Threat of Mobile Communication Network

可能导致对 WAP 网关系统产生危害的不希望事件潜在起因，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。常见的 WAP 网关系统络威胁有外部攻击、链路设备节点失效、火灾、水灾等等。

3.1.9

WAP网关系统脆弱性 Vulnerability of Mobile Communication Network

脆弱性是WAP网关系统中存在的弱点、缺陷与不足，不直接对资产造成危害，但可能被威胁所利用从而危及资产的安全。

3.1.10

WAP网关系统灾难 Disaster of Mobile Communication NETWORK

由于各种原因，造成WAP网关系统故障或瘫痪，使WAP网关系统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。

3.1.11

WAP网关系统灾难备份 Backup for Disaster Recovery of Mobile Communication Network

为了WAP网关系统灾难恢复而对相关网络要素进行备份的过程。

3.1.12

WAP网关系统灾难恢复 Disaster Recovery of Mobile Communication Network

为了将WAP网关系统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。

3.1.13

WAP网关系统相关系统 Systems of Mobile Communication Network

组成WAP网关系统的相关系统，包括移动通信网中的核心网络设备，以及计费系统、网管系统。

3.1.14

访谈 Interview

检测人员通过与WAP网关系统有关人员（个人/群体）进行交流、讨论等活动，查看WAP网关系统安全等级保护、WAP网关系统安全风险评估和WAP网关系统灾难备份及恢复相关措施的落实情况以及相关工作的开展情况的一种方法。

3.1.15

检查 Examination

检测人员通过对检测对象进行观察、查验和分析等活动，获取证据以检查安全等级保护、安全风险评估、灾难备份及恢复相关措施的落实情况以及相关工作开展情况的一种方法。

3.1.16

测试 Testing

检测人员通过对检测对象按照预定的方法/工具使其产生特定行为的活动，查看、分析输出结果，获取证据以证明WAP网关系统安全等级保护措施、WAP网关系统风险评估措施和WAP网关系统灾难备份及恢复措施是否有效的一种方法。

3.2 缩略语

下列缩略语适用于本标准。

GGSN	Gateway GPRS Support Node	关口GPRS支持节点
PDSN	Packet Data Service Node	分组数据服务节点
PI	Push Initiator	push发起者
PPG	Push Proxy Gateway	Push代理网关
SSL	Secure Sockets Layer	套接字安全层
SP	Service Provider	服务提供商
IP	Internet Protocol	因特网协议
TLS	Transport Layer Security	传输层安全
VPN	Virtual Private Network	虚拟专用网
WAP	Wireless Application Protocol	无线应用协议
WTLS	Wireless Transport Layer Security	无线传输层安全

4 WAP 网关系统安全防护检测概述

4.1 安全防护检测范围

WAP网关安全防护检测范围包括WAP代理网关、Push代理网关（PPG）、数据库、安全设备（如防火墙）及其他服务器（如统计分析服务器）等。

4.2 安全防护检测对象

一个WAP网关系统覆盖的业务区域可能是一个省/市，或多个省，可将WAP网关系统作为一个定级对象。

安全等级保护的检测对象确定以后，风险评估的检测对象、灾难备份及恢复检测的检测对象应与安全定级保护的检测对象相一致。

4.3 安全防护检测内容

按照WAP网关系统安全防护检测的需要，将WAP网关系统安全防护检测分为WAP网关系统风险评估检测、WAP网关系统安全等级保护检测和WAP网关系统灾难备份及恢复检测等3个部分。

WAP网关系统安全防护检测内容包括以下一些内容：

——WAP网关系统安全风险评估检测

主要包括风险评估范围、风险评估内容检测、风险评估要素检测、风险评估赋值原则检测、风险评估计算方法检测、风险评估文件类型检测和风险评估文件记录检测等；

——WAP网关系统安全等级保护检测

主要包括业务安全检测、网络安全检测、设备安全检测、物理安全检测、管理安全检测等；

——WAP网关系统灾难备份及恢复检测

主要包括冗余系统、冗余设备及冗余链路检测、冗余路由检测、备份数据检测、技术支持能力检测、运行维护管理检测和灾难恢复预案检测等。

4.4 安全防护检测结果判定

WAP网关系统安全防护检测包括对WAP网关系统的安全风险评估、安全等级保护、灾难备份及恢复3个部分的检测，应对3个部分的检测结果分别进行判定，并根据检测结果分别出具检测报告，检测报告中应具体说明安全防护工作的优势和不足。

对每一个部分中的每一个测试项，应根据具体实施情况进行等级化评价（分5级：很好、较好、一般、较差、很差）。参照表1将各测试项的评价等级换算成评分，各测试项的分数经过一定的算法（例如加权平均）分别得到安全等级保护、安全风险评估、灾难备份及恢复3个部分的总分数，根据总分数分别对安全等级保护、安全风险评估、灾难备份及恢复3个部分的检测结果进行等级化评定，总分数和评定等级的关系如表2所示。在计算总分数过程中，应充分考虑到各测试项在安全防护检测要求中所占的比重，例如，表3给出了安全等级保护子类所占的比重。WAP网关系统安全防护检测的结果还应充分考虑到支持WAP网关系统运行的各相关系统的检测结果。

表1 测试项评分方法

评价结果	评分
实施很好	5
实施较好	4
实施一般	3
实施较差	2
实施很差	1

表2 总分数和评定等级的关系

总分数x	评定等级
$X \geq 4.5$	很好
$3.5 \leq x < 4.5$	较好
$2.5 \leq x < 3.5$	一般
$1.5 \leq x < 2.5$	较差
$x < 1.5$	很差

表3 安全等级保护子类所占的比重

比重（%）	安全等级保护子类
20	业务安全
20	网络安全
10	设备安全
10	物理环境安全
40	管理安全

5 WAP 网关系统安全等级保护检测要求

5.1 第 1 级检测要求

不作要求。

5.2 第 2 级检测要求

5.2.1 业务安全

(1) 检测方式

访谈，检查，并通过测试工具进行测试。

(2) 检测对象

设备运行日志，网络管理系统日志、用户投诉及处理记录，故障记录，SP 业务管理资料。

(3) 检测实施

a) 应访谈业务系统管理人员，并查看业务运营的历史记录，业务系统升级相关资料等检查网络是否能够保证在运行的系统上引入新业务、升级业务或者升级系统时不会引起网络所提供业务的中断或系统瘫痪；

b) 应访谈相关技术人员，并通过测试工具验证非法PI（Push发起者）能否接入PPG服务器，能否发起Push消息；

c) 应询问相关业务系统管理人员并检查业务运营的历史记录及SP业务管理资料，检查是否有针对SP各类业务的业务规范，在SP开通业务前是否对SP进行了测试验证；

d) 检查SP业务管理资料，验证SP是否具有服务的资质备案。

5.2.2 网络安全

5.2.2.1 网络拓扑结构

(1) 检测方式

访谈，检查。

(2) 检测对象

网络拓扑结构，网络拓扑图，网络设计/验收文档，网管系统，设备运行日志，网络设备。

(3) 检测实施

a) 应访谈网络管理人员，查看网络设计/验收文档，查看实际的网络设备运行日志、故障记录、用户投诉及处理记录，查看网络设备处理能力是否具备冗余空间，不能由于设备配置不够而导致网络全部或者局部瘫痪，负荷设计的水平是否满足流量高负荷时需求，是否形成单点故障，节假日突发话务量是否会影响网络；

b) 应访谈 WAP 网关系统管理人员，查看 WAP 网关系统网络拓扑图，了解目前 WAP 网关系统的网

络组织情况，查看其与当前运行情况是否一致。

5.2.2.2 网络安全协议

(1) 检测方式

访谈，或通过测试工具、仪表进行验证、检查。

(2) 检测对象

系统设计文档，设备后台运行日志，网络设备。

(3) 检测实施

a) 应访谈网络管理人员，查看网络设计/验收文档和入网测试报告，查看设备运行日志，或者通过仪表验证，查看 WAP 终端与 WAP 网关之间是否可以进行 WTLS 连接，使用协议抓包软件测试 WAP 终端与 WAP 网关之间是否进行了 WTLS 协议过程；

b) 应访谈网络管理人员，查看网络设计/验收文档和入网测试报告，查看设备运行日志，或者通过仪表验证，通过 WAP 终端访问 HTTPS 安全网站，从测试仪表或协议抓包软件验证 WAP 终端与应用服务器之间是否能够建立 TLS 连接。

5.2.2.3 访问控制安全

(1) 检测方式

访谈，检查。

(2) 检测对象

网络设计/验收文档，网管系统，设备运行日志，后台操作维护系统，网络设备。

(3) 检测实施

应访谈网络管理人员，查看网络设计/验收文档和入网测试报告，查看设备运行日志，查看后台操作维护系统是否提供访问控制功能，是否设置了不同的访问角色。

5.2.2.4 网络攻击防范

(1) 检测方式

访谈，检查。

(2) 检测对象

网络设计/验收文档，网管系统，设备运行日志，后台操作维护系统，网络设备。

(3) 检测实施

应访谈网络管理员，查看网络拓扑结构图，查看系统设计文档，并询问相关系统管理人员，是否在 WAP 网关系统与外部系统间设置了防火墙，防火墙策略设置是否合理。

5.2.2.5 安全审计

(1) 检测方式

访谈，检查。

(2) 检测对象

网络设计/验收文档，网管系统，设备运行日志，网络设备。

(3) 检测实施

应访谈网络管理人员，查看网络设计/验收文档和入网测试报告，查看设备运行日志，查看系统是否对系统管理员的登录、操作记录进行了记录，审计日志的保存期是否满足《移动上网日志留存规范》第

6 章的要求。

5.2.3 设备安全

(1) 检测方式

访谈, 检查。

(2) 检测对象

设备入网检测报告, 设备入网证, 安全检测报告。

(3) 检测实施

应访谈相关技术支持人员和管理人员, 查看设备是否有入网检测报告、设备入网证、安全检测报告等。

5.2.4 物理环境安全

(1) 检测方式

访谈, 检查。

(2) 检测对象

机房、办公场地, 设计/验收文档。

(3) 检测实施

除应满足 YD/T 1755—2008 中第 2 级的检测要求外, 还应满足:

- a) 访谈物理安全负责人, 查看机房设计文档, 检查机房整体抗震能力应不低于里氏 7 级;
- b) 访谈物理安全负责人, 查看机房管理制度文档, 查看机房现场, 检查机房是否具备防虫防鼠等相关措施, 以有效防范鼠虫蚁害。

5.2.5 管理安全

应满足 YD/T 1757—2008 中第 2 级的检测要求。

5.3 第 3.1 级检测要求

5.3.1 业务安全

(1) 检测方式

访谈, 或通过测试工具、仪表进行验证、检查。

(2) 检测对象

系统设计文档, 设备运行日志, 网络管理系统日志、用户投诉及处理记录, 操作管理后台系统。

(3) 检测实施

除满足 5.2.1 的要求外, 还应该满足:

- a) 访谈网络管理人员, 查看网络设计/验收文档和入网测试报告, 查看设备运行日志, 查看系统后台操作管理界面, 验证系统是否对 PI 的 IP 地址、域名等信息进行白名单控制, 验证不在白名单中的 IP 地址是否能成功发送 Push 消息;
- b) 访谈网络管理人员, 查看网络设计/验收文档和入网测试报告, 查看设备运行日志, 查看系统后台操作管理界面, 验证系统是否对 PI 发送的 Push 消息频率、条数等进行控制, 验证是否能发送超过系统设置最多条数的 Push 消息;
- c) 访谈网络管理人员, 通过测试工具验证 WAP 网关系统是否对 Push 消息的大小进行了限制, 验证 WAP 网关系统是否能阻止超大 Push 消息的发送;

d) 访谈网络管理人员, 查看网络设计/验收文档和入网测试报告, 查看设备运行日志, 查看系统后台操作管理界面, 通过测试软件验证是否能使用 WAP 网关代理功能发送 Push 消息;

e) 访谈网络管理人员, 使用测试工具, 验证 WAP 网关系统是否能对终端用户所发起的访问请求数据包进行识别, 能识别测试工具发起的超长/畸形数据包, 并进行自动过滤;

f) 访谈网络管理员, 使用测试工具, 验证 WAP 网关系统能否对终端用户所发起的访问目标服务器进行识别, 是否能防止测试工具将 WAP 网关作为跳板访问电信网内服务器。

5.3.2 网络安全

5.3.2.1 网络拓扑结构

(1) 检测方式

访谈, 检查。

(2) 检测对象

网络拓扑结构, 网络拓扑图, 网络设计/验收文档, 网管系统, 设备运行日志, 故障记录, 网络设备。

(3) 检测实施

同5.2.2.1的要求。

5.3.2.2 网络安全协议

(1) 检测方式

访谈检查, 或通过测试工具、仪表进行验证。

(2) 检测对象

系统设计文档, 设备后台运行日志, 网络设备。

(3) 检测实施

同 5.2.2.2 的要求。

5.3.2.3 访问控制安全

(1) 检测方式

访谈, 或通过测试工具、仪表进行验证、检查。

(2) 检测对象

网络设计/验收文档, 网管系统, 设备运行日志, 后台操作维护系统, 网络设备。

(3) 检测实施

除满足 5.2.2.3 的要求外, 还应该满足:

a) 访谈网络管理人员, 查看网络设计/验收文档和入网测试报告, 查看设备运行日志, 查看后台操作维护系统是否设置了不同的角色, 不同角色是否设置了不同的权限, 是否设置了多级密码;

b) 访谈网络管理人员, 查看网络设计/验收文档和入网测试报告, 查看设备运行日志, 查看后台操作维护系统是对远程登录访问是否使用了 VPN 或其他安全接入认证方式, 用测试仪器或协议抓包软件测试验证远程操作维护的数据流是否进行了加密;

c) 访谈网络管理人员, 查看网络设计/验收文档和入网测试报告, 查看设备运行日志, 查看后台操作维护系统是否对远程操作维护进行单独审计, 对远程操作维护的操作内容是否进行了记录与存储。

5.3.2.4 安全审计

(1) 检测方式

访谈，检查。

(2) 检测对象

网络设计/验收文档，网管系统，设备运行日志，网络设备。

(3) 检测实施

同 5.2.2.4 的要求。

5.3.2.5 网络攻击防范

(1) 检测方式

访谈，或通过测试工具、仪表进行验证、检查。

(2) 检测对象

网络设计/验收文档，网管系统，设备运行日志，网络设备。

(3) 检测实施

a) 应访谈网络管理员，查看网络拓扑结构图，查看系统设计文档，并询问相关系统管理人员，查看验证防火墙是否能够根据访问请求的源 IP 地址溯源到内网用户手机 IP 地址；

b) 应访谈网络管理员，查看网络拓扑结构图，查看系统设计文档，并询问相关系统管理人员，查看系统内基于 Windows 操作系统的网络是否部署了网络入侵检测系统，并能及时处理入侵的报警；

c) 应访谈网络管理员，查看系统漏洞扫描记录，验证系统是否每 3 个月进行一次网络安全漏洞扫描，形成相关记录文档，并根据扫描的结果更正网络安全漏洞和系统中的错误配置；

d) 应访谈网络管理员，查看用户投诉及处理记录、故障记录，并现场使用测试工具，验证系统是否配置了能够抵御 Dos/DDos 攻击的相应措施。

5.3.2.6 数据存储安全

(1) 检测方式

访谈，检查。

(2) 检测对象

网络设计/验收文档，网管系统，设备运行日志，网络设备。

(3) 检测实施

访谈网络管理人员，查看网络设计/验收文档和入网测试报告，查看设备运行日志，查看 WAP 网关系统是否对用户访问业务数据、业务信息、话单信息等数据进行了存储和数据备份。日志备份应满足《移动上网日志留存规范》第 6 章的要求。

5.3.3 设备安全

(1) 检测方式

访谈，检查和使用测试工具进行测试。

(2) 检测对象

网络设计/验收文档，网管系统，设备运行日志，网络设备。

(3) 检测实施

除满足 5.2.3 的要求之外，还应该满足：

a) 访谈网络管理员，查看网络拓扑结构图，查看系统设计文档，并询问相关系统管理人员，查看 WAP 网关关键设备是否进行了负载均衡配置；

b) 访谈网络管理员，查看用户投诉及处理记录、故障记录，并现场使用测试工具，验证系统内服务器是否关闭了不必要的端口及服务，是否安装不必要的软件；

c) 访谈网络管理员，查看网络拓扑结构图，查看系统设计文档，并询问相关系统管理人员，查看系统内基于 Windows 操作系统的主机是否具备防病毒软件。防病毒软件是否能定期进行病毒库的升级，系统病毒库是否为防病毒厂商发布的最新病毒库版本；

d) 访谈网络管理员，查看系统漏洞扫描记录，验证是否每 3 个月对系统内服务器进行一次安全漏洞扫描，形成相关记录文档，并根据扫描的结果更正服务器安全漏洞和系统中的错误配置。

5.3.4 物理环境安全

(1) 检测方式

访谈，检查。

(2) 检测对象

机房、办公场地，设计/验收文档。

(3) 检测实施

除满足YD/T 1755—2008中第3.1级的检测要求外，还应满足：

a) 访谈物理安全负责人，查看机房设计文档，检查机房整体抗震能力应不低于里氏8级；

b) 访谈物理安全负责人，查看机房管理制度文档，查看机房现场，检查机房是否具备防虫防鼠等相关措施，以有效防范鼠虫蚁害。

5.3.5 管理安全

应满足YD/T 1757—2008中第3.1级的检测要求。

5.4 第 3.2 级检测要求

5.4.1 业务安全

应满足5.3.1的要求。

5.4.2 网络安全

应满足5.3.2的要求。

5.4.3 设备安全

应满足5.3.3的要求。

5.4.4 物理环境安全

应满足YD/T 1755—2008中第3.2级的检测要求。

5.4.5 管理安全

应满足YD/T 1757—2008中第3.2级的安全要求。

5.5 第 4 级检测要求

同第3.2级要求。

5.6 第 5 级检测要求

待补充。

6 WAP 网关系统安全风险评估检测要求

6.1 安全风险评估范围

(1) 检测方式

访谈，检查。

(2) 检测对象

风险评估报告。

(3) 检测实施

应访谈风险评估负责人，询问进行WAP网关系统风险评估时，选择的风险评估范围；检查风险评估报告，查看WAP网关系统风险评估范围是否与要求一致。

6.2 安全风险评估内容

(1) 检测方式

访谈，检查。

(2) 检测对象

风险评估报告。

(3) 检测实施

a) 应访谈WAP网关系统风险评估负责人、查看风险评估报告，检查WAP网关系统风险评估是否覆盖了技术安全和管理安全；

b) 应访谈WAP网关系统风险评估负责人、查看风险评估报告，检查WAP网关系统风险评估中技术安全是否覆盖了业务安全、网络安全、设备安全和物理环境安全等方面；

c) 应访谈WAP网关系统风险评估负责人、查看风险评估报告，检查WAP网关系统风险评估中管理安全是否覆盖了安全管理机构、安全管理制度、人员安全管理、安全建设管理、安全运维管理等方面。

6.3 安全风险评估要素

(1) 检测方式

访谈，检查。

(2) 检测对象

风险评估报告。

(3) 检测实施

a) 应访谈风险评估负责人，询问进行WAP网关系统风险评估时采用了哪些风险评估的要素；查看风险评估报告，检查WAP网关系统风险评估时是否包含了资产、脆弱性、威胁、安全措施、风险和残余风险等要素；

b) 应访谈风险评估负责人，询问进行WAP网关系统风险评估时考虑了哪些风险评估要素的相关属性；查看风险评估报告，检查WAP网关系统风险评估报告时是否包含了与评估要素密切相关的业务战略、资产价值、安全需求和安全事件等属性；

c) 应访谈风险评估负责人，询问进行WAP网关系统风险评估时评估了哪些资产；查看风险评估报告，检查WAP网关系统风险评估时的资产是否包含了WAP网关、Push代理网关（PPG）、数据库、安全设备（如防火墙）及其他服务器（如统计分析服务器）等；是否包含了物理环境设备，包括机房、电力供应系统，电磁防护系统、防火、防水和防潮系统、防静电系统、防雷击系统、温湿度控制系统等，各种设备的系统软件，设备中的重要数据，网络提供的各类业务，设备维护人员、各种管理规定和设备文档等；

d) 应访谈风险评估负责人, 询问计算WAP网关系统各资产的资产价值时考虑了哪些因素; 查看风险评估报告, 检查WAP网关系统风险评估中, 计算各资产的资产价值是否主要考虑了社会影响力、资产价值和可用性等因素, 同时采用了合理的计算方法;

e) 应访谈风险评估负责人, 询问识别了WAP网关系统各资产的脆弱性时考虑了哪些方面的脆弱性; 查看风险评估报告, 检查WAP网关系统风险评估中脆弱性识别是否包含了技术脆弱性和管理脆弱性等方面;

f) 应访谈风险评估负责人, 询问识别了WAP网关系统各资产的脆弱性时考虑了哪些方面的脆弱性; 查看风险评估报告, 检查WAP网关系统风险评估中技术脆弱性是否包含了业务/应用脆弱性、网络脆弱性、设备脆弱性和物理环境脆弱性; 管理脆弱性是否包含安全管理机构方面的脆弱性、人员安全管理方面脆弱性、建设管理方面的脆弱性、运维管理方面的脆弱性。

g) 应访谈风险评估负责人, 询问对WAP网关系统存在哪些威胁; 查看风险评估报告, 检查WAP网关系统风险评估时威胁识别是否包含了环境威胁、人员威胁;

h) 应访谈风险评估负责人, 询问威胁识别依据了哪些历史数据; 查看风险评估报告, 检查WAP网关系统风险评估中威胁识别是否依据了已有安全事件报告数据、检测工具检测数据和国内外同行业报告数据等多个方面;

i) 应访谈风险评估负责人, 询问风险值的计算采用了哪种计算方法; 查看风险评估报告, 检查WAP网关系统风险评估中风险值的计算是否主要考虑了资产、威胁和脆弱性等因素, 是否采用了合理的计算方法;

j) 应访谈风险评估负责人, 询问如何确定的风险阈值; 查看风险评估报告, 检查WAP网关系统风险评估中确定的风险阈值是否合理, 是否与资产所在网络或系统的安全等级相结合;

k) 应访谈风险评估负责人, 询问对于不可接收的风险, 是否制定了相应的风险处理计划; 查看风险评估报告, 检查WAP网关系统风险评估中对于不可接受的风险, 是否制定了相应的风险处理计划, 采用风险处理计划以后, 风险值是否满足阈值要求。

6.4 安全风险评估赋值原则

(1) 检测方式

访谈, 检查。

(2) 检测对象

风险评估报告。

(3) 检测实施

a) 应访谈风险评估负责人, 询问WAP网关系统风险评估时对资产的赋值遵循的原则; 查看风险评估报告, 检查WAP网关系统各资产的赋值是否从资产的社会影响力、资产价值和可用性3个方面和5个等级进行赋值;

b) 应访谈风险评估负责人, 询问WAP网关系统风险评估时对脆弱性的赋值遵循的原则; 查看风险评估报告, 检查WAP网关系统脆弱性的赋值是否考虑赋值对象对资产损害程度等因素, 同时是否按照5个等级进行赋值;

c) 应访谈风险评估负责人, 询问WAP网关系统风险评估时对威胁的赋值遵循的原则; 查看风险评估报告, 检查WAP网关系统威胁的赋值是否依据威胁发生的频率, 同时是否按照5个等级进行赋值。

6.5 安全风险评估计算方法

(1) 检测方式

访谈，检查。

(2) 检测对象

风险评估报告。

(3) 检测实施

a) 应访谈风险评估负责人，询问WAP网关系统风险评估中采用了什么样的方法计算资产价值；查看风险评估报告，检查WAP网关系统资产价值的计算方法是否合理，是否有对于所采用计算方法的理论分析；

b) 应访谈风险评估负责人，询问WAP网关系统风险评估中采用了什么样的方法计算风险值；查看风险评估报告，检查WAP网关系统风险值的计算方法是否合理，是否具有对于所采用计算方法的理论分析。

6.6 安全风险评估文件类型

(1) 检测方式

访谈，检查。

(2) 检测对象

风险评估方案，风险评估程序，资产识别清单，重要资产清单，脆弱性列表，威胁列表，已有安全措施确认表，风险评估报告，风险评估记录，风险处理计划等风险评估文件。

(3) 检测实施

a) 应访谈风险评估负责人，询问是否制定了风险评估方案；查看此文件，检查是否包括风险评估的目标、范围、人员、评估方法、评估结果的形式和实施进度等内容；

b) 应访谈风险评估负责人，询问是否制定了风险评估程序；查看此文件，检查是否包括风险评估的目的、职责、过程、相关的文件要求，以及实施本次评估所需要的各种资产、威胁、脆弱性识别和判断依据等内容；

c) 应访谈风险评估负责人，询问是否制定了资产识别清单；查看此文件，检查是否根据组织在风险评估程序文件中所确定的资产分类方法进行资产识别，形成资产识别清单，明确资产的责任人/部门等内容；

d) 应访谈风险评估负责人，询问是否制定了重要资产清单；查看此文件，检查是否根据资产识别和赋值的结果，形成重要资产列表，包括重要资产名称、描述、类型、重要程度、责任人/部门等内容；

e) 应访谈风险评估负责人，询问是否根据威胁识别和赋值的结果，制定了威胁列表；查看此文件，检查是否包括威胁名称、种类、来源、动机及出现的频率等内容；

f) 应访谈风险评估负责人，询问是否根据脆弱性识别和赋值的结果，形成脆弱性列表；查看此文件，检查是否包括具体脆弱性的名称、描述、类型及严重程度等；

g) 应访谈风险评估负责人，询问是否根据已采取的安全措施确认的结果，形成已有安全措施确认表；查看此文件，检查是否包括已有安全措施名称、类型、功能描述及实施效果等；

h) 应访谈风险评估负责人, 询问是否有风险评估报告; 查看此文件, 检查是否对整个风险评估过程和结果进行总结, 详细说明被评估对象, 风险评估方法, 资产、威胁、脆弱性的识别结果, 风险分析、风险统计和结论等内容;

i) 应访谈风险评估负责人, 询问是否有风险处理计划; 查看此文件, 检查是否对评估结果中不可接受的风险制定风险处理计划, 选择适当的控制目标及安全措施, 明确责任、进度、资源, 并通过对残余风险的评价以确定所选择安全措施的有效性;

j) 应访谈风险评估负责人, 询问是否有风险评估记录; 查看此文件, 检查风险评估过程中的各种现场记录是否可复现评估过程, 是否能够作为产生歧义后解决问题的依据。

6.7 安全风险评估文件记录

(1) 检测方式

访谈, 检查。

(2) 检测对象

风险评估方案, 风险评估程序, 资产识别清单, 重要资产清单, 脆弱性列表, 威胁列表, 已有安全措施确认表, 风险评估报告, 风险评估记录, 风险处理计划等风险评估文件。

(3) 检测实施

a) 应访谈风险评估负责人, 询问风险评估文件正式确认前是否需要批准; 应查看风险评估文件, 检查文件正式确认前是否得到批准;

b) 应访谈风险评估负责人, 询问风险评估文件的更改和现行修订状态是如何进行识别的; 应查看风险评估文件, 检查文件的更改和现行修订状态是否是可识别的;

c) 应访谈风险评估负责人, 询问风险评估文件的版本如何管理; 应查看风险评估文件, 检查是否有版本划分以及相应的版本使用说明;

d) 应访谈风险评估负责人, 询问作废文件是如何管理的; 应查看风险评估文件, 检查是否对于作废文件作了标识;

e) 应访谈风险评估负责人, 询问如何对文件进行控制; 应查看风险评估文件, 检查是否规定其标识、储存、保护、检索、保存期限以及处置所需的控制。

7 WAP 网关系统灾难备份及恢复检测要求

7.1 第 1 级检测要求

不作要求。

7.2 第 2 级检测要求

7.2.1 冗余系统、冗余设备及冗余链路

(1) 检测方式

访谈, 检查。

(2) 检测对象

冗余系统、冗余设备和冗余链路, 运行日志、故障记录, 设计/验收文档, 演练文档。

(3) 检测实施

a) 应访谈安全管理人员, 询问并现场查看采取了哪些措施防止单节点的灾难导致其他节点的业务提供发生异常, 查看运行日志、故障记录, 查看是否发生过单一地区范围的灾难导致其他地区的业务提供发生异常的情况, 安全措施是否与设计/验收文档相符合;

b) 应访谈安全管理人员, 查看演练文档, 查看 WAP 网关系统的网络灾难演练恢复时间是否能够满足行业管理、网络和业务运营商应急预案的相关要求。

7.2.2 冗余路由

(1) 检测方式

访谈, 检查。

(2) 检测对象

冗余路由, 设计/验收文档, 演练记录, 历史记录。

(3) 检测实施

应访谈安全管理人员, 查看设计/验收文档和历史记录, 询问GGSN/PDSN至WAP网关系统设备之间的路由具有负荷分担方式, WAP网关系统和IP网之间的路由支持冗余方式, 查看其冗余负荷分担、冗余路由是否与设计一致。

7.2.3 备份数据

(1) 检测方式

访谈, 检查。

(2) 检测对象

数据备份服务器, 设计/验收文档, 演练历史记录。

(3) 检测实施

a) 应访谈安全管理人员, 询问并查看数据备份服务器, 查看WAP网关系统中关键数据(如计费数据、用户数据、网络配置数据、管理员操作维护记录)本地备份的情况;

b) 应访谈安全管理人员, 询问并查看数据备份服务器、演练记录, 查看WAP网关系统关键数据是否具备数据恢复能力, 了解备份范围和时间间隔、采取的备份方式。

7.2.4 人员和技术支持能力

(1) 检测方式

访谈, 检查。

(2) 检测对象

负责灾难备份及恢复的管理人员, 历史值班记录。

(3) 检测实施

应访谈安全管理相关人员, 询问并查看历史值班记录, 查看是否有负责灾难备份及恢复的机房管理人员。

7.2.5 运行维护管理能力

(1) 检测方式

访谈, 检查。

(2) 检测对象

机房运行管理制度，介质存取、验证和转储管理制度，设备和网络运行管理制度，数据容灾备份管理制度，联络和协作的记录。

(3) 检测实施

a) 应访谈安全管理人员，询问并查看机房运行管理制度，查看是否有完善的针对灾难备份及恢复的机房运行管理制度；

b) 应访谈安全管理人员，询问并查看介质存取、验证和转储管理制度，查看是否有完善的针对灾难备份及恢复的介质存取、验证和转储管理制度，查看备份数据的授权访问情况。

7.2.6 灾难恢复预案

(1) 检测方式

访谈，检查。

(2) 检测对象

灾难恢复预案，设计/验收文档。

(3) 检测实施

应访谈安全管理人员，询问并查看灾难恢复预案，查看WAP网关系统是否具有完整的灾难恢复预案，是否与设计/验收文档一致。

7.3 第3.1级检测要求

除满足7.1中要求外，还需满足下列要求。

7.3.1 冗余系统、冗余设备及冗余链路

应满足7.2.1的要求。

7.3.2 冗余路由

(1) 检测方式

访谈，检查。

(2) 检测对象

冗余路由，设计/验收文档，演练记录，历史记录，传送链路。

(3) 检测实施

除满足7.2.2的要求外，还需满足：

应访谈安全管理人员，检查设计/验收文档和历史记录，查看WAP网关系统是否采用了流量负荷分担方式。

7.3.3 备份数据

(1) 检测方式

访谈，检查。

(2) 检测对象

数据备份服务器，设计/验收文档，演练历史记录。

(3) 检测实施

除满足7.2.3的要求外，还需满足：

应访谈安全管理人员，询问并查看数据备份服务器，查看WAP网关系统中关键数据（如计费数据、网络配置数据）在不同的地理位置进行备份的情况。

7.3.4 人员和技术支持能力

(1) 检测方式

访谈，检查。

(2) 检测对象

负责灾难备份及恢复的技术人员，历史值班记录，培训记录。

(3) 检测实施

除满足7.2.4的要求外，还需满足：

a) 访谈安全管理相关人员，询问并查看历史值班记录，检查是否有负责灾难备份及恢复的技术人员，检查相关人员对灾难备份及恢复的技术能力；

b) 访谈安全管理相关人员，询问并查看培训记录，查看负责灾难备份及恢复的人员定期进行灾难备份及恢复方面的技能培训的情况。

7.3.5 运行维护管理能力

(1) 检测方式

访谈，检查。

(2) 检测对象

设备和网络运行管理制度，数据异地容灾备份管理制度，联络和协作的记录。

(3) 检测实施

除满足7.2.5的要求外，还需满足：

a) 访谈安全管理人员，询问并查看设备和网络运行管理制度，查看是否有完善的针对灾难备份及恢复的设备和网络运行管理制度；

b) 访谈安全管理人员，询问并查看数据异地容灾备份管理制度，查看是否有完善的针对灾难备份及恢复的数据异地容灾备份管理制度；

c) 访谈安全管理人员，询问并查看与其他组织进行联络和协作的记录，查看WAP网关系统内部是否具有与外部组织保持良好的联络和协作的能力。

7.3.6 灾难恢复预案

(1) 检测方式

访谈，检查

(2) 检测对象

灾难恢复预案，设计/验收文档，灾难恢复预案的教育和培训记录、演练记录、调整记录、管理制度。

(3) 检测实施

除满足7.2.6的要求外，还需满足：

a) 访谈安全管理人员，询问并查看灾难恢复预案的教育和培训记录，查看对灾难恢复预案进行教育和培训的情况，是否达到了教育和培训的预期目标，查看相关人员对灾难恢复预案的了解情况，查看相关人员是否具有对灾难恢复预案进行实际操作的能力；

b) 访谈安全管理人员，询问并查看灾难恢复预案演练记录，查看灾难恢复预案的演练情况，灾难恢复预案演练的效果是否达到设计要求；查看灾难恢复预案调整记录，查看根据演练结果对灾难恢复预案进行修正的情况。

7.4 第 3.2 级检测要求

7.4.1 冗余系统、冗余设备及冗余链路

应满足7.3.1的要求。

7.4.2 冗余路由

应满足7.3.2的要求。

7.4.3 备份数据

应满足7.3.3的要求。

7.4.4 人员和技术支持能力

应满足7.3.4的要求。

7.4.5 运行维护管理能力

应满足7.3.5的要求。

7.4.6 灾难恢复预案

(1) 检测方式

访谈，检查。

(2) 检测对象

灾难恢复预案，设计/验收文档，灾难恢复预案的管理制度。

(3) 检测实施

除满足7.3.6的要求外，还需满足：

访谈安全管理人员，询问并查看WAP网关系统管理制度，查看是否有灾难恢复预案的管理制度。

7.5 第 4 级检测要求

同第3.2级要求。

7.6 第 5 级检测要求

待补充。

参 考 文 献

YD/T 1728-2008	电信网和互联网安全防护管理指南
YD/T 1729-2008	电信网和互联网安全等级保护实施指南
YD/T 1731-2008	电信网和互联网安全风险评估实施指南
YD/T 1731-2008	电信网和互联网灾难备份及恢复实施指南

中华人民共和国
通信行业标准
WAP 网关系统安全防护检测要求
YD/T 2242-2011

*

人民邮电出版社出版发行
北京市崇文区夕照寺街 14 号 A 座
邮政编码：100061
宝隆元（北京）印刷技术有限公司印刷
版权所有 不得翻印

*

开本：880×1230 1/16 2011 年 9 月第 1 版
印张：1.75 2011 年 9 月北京第 1 次印刷
字数：43 千字

ISBN 978 - 7 - 115 - 2408/ 11 - 359

定价：20 元

本书如有印装质量问题，请与本社联系 电话：(010)67114922