

ICS 33.040

M 10

YD

中华人民共和国通信行业标准

YD/T 2697-2014

公众无线局域网安全防护检测要求

Security protection test requirements for
public wireless local area network

2014-10-14 发布

2014-10-14 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 | 4 |
| 4 PWLAN 安全防护检测概述 | 5 |
| 4.1 PWLAN 安全防护检测内容 | 5 |
| 4.2 PWLAN 安全防护检测对象 | 5 |
| 4.3 PWLAN 安全防护检测环境 | 5 |
| 5 PWLAN 安全防护检测要求 | 6 |
| 5.1 第 1 级要求 | 6 |
| 5.2 第 2 级要求 | 28 |
| 5.3 第 3 级要求 | 41 |
| 5.4 第 4 级要求 | 41 |
| 5.5 第 5 级要求 | 41 |

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，该系列标准的结构及名称预计如下：

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》
51. 《移动互联网应用安全防护要求》
52. 《移动互联网应用安全防护检测要求》
53. 《公众无线局域网安全防护要求》
54. 《公众无线局域网安全防护检测要求》(本标准)
55. 《电信网和互联网安全防护基线配置要求及检测要求 网络设备》
56. 《电信网和互联网安全防护基线配置要求及检测要求 安全设备》
57. 《电信网和互联网安全防护基线配置要求及检测要求 操作系统》
58. 《电信网和互联网安全防护基线配置要求及检测要求 数据库》
59. 《电信网和互联网安全防护基线配置要求及检测要求 中间件》
60. 《电信网和互联网安全防护基线配置要求及检测要求 WEB应用系统》
61. 《电信和互联网用户个人信息保护通用技术要求和管理工作要求》
62. 《电信和互联网用户个人信息保护检测要求》

本标准与YD/T 2696-2014《公众无线局域网安全防护要求》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。

本标准按照GB/T1.1-2009给出的规则起草。

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、中国联合网络通信集团有限公司、中国电信集团公司、中国移动通信集团公司、北京启明星辰信息技术股份有限公司。

本标准主要起草人：张彦超、谢 玮、龚双瑾、卜 哲、廖 璇、魏 薇、封 莎、崔 涛、杨淑敏、张佳琦、王新峰、陈 军、杨晓光、李祥军、崔 鹏。

公众无线局域网安全防护检测要求

1 范围

本标准规定了公众无线局域网分安全保护等级的安全防护检测要求,涉及到业务安全、设备及软件系统安全、网络安全、物理环境安全和管理安全。

本标准适用于基础电信业务经营者和增值电信业务经营者建设或者运营的公众无线局域网。

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 1731-2008 《电信网和互联网灾难备份及恢复实施指南》
- YD/T 1754-2008 《电信网和互联网物理环境安全等级保护要求》
- YD/T 1756-2008 《电信网和互联网管理安全等级保护要求》
- YD/T 2698-2014 《电信网与互联网安全防护基线配置要求及检测要求 网络设备》
- YD/T 2700-2014 《电信网与互联网安全防护基线配置要求及检测要求 数据库》
- YD/T 2701-2014 《电信网与互联网安全防护基线配置要求及检测要求 操作系统》

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文件。

3.1.1

无线局域网 Wireless Local Area Networks

采用无线工作方式,空中接口采用载波侦听多路访问/碰撞避免(CSMA/CA)技术实现共享媒质接入控制的一种局域网技术。无线局域网只涉及空中接口的物理层(PHY)和媒质接入控制层(MAC),对上层协议透明。无线局域网一般工作在2.4GHz或5.8GHz频段。在本标准中,无线局域网指空中接口采用IEEE802.11标准族规定的空中接口协议。

3.1.2

公众无线局域网 Public Wireless Local Area Networks

利用无线局域网(WLAN)、IP、Web等技术组建并为公众提供网络接入服务的网络。

3.1.3

公众无线局域网安全等级 Security Classification of Public Wireless Local Area Network

公众无线局域网安全重要程度的表征。重要程度可从公众无线局域网受到破坏后,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。

3.1.4

公众无线局域网安全等级保护 Classified Security Protection of Public Wireless Local Area Network

对公众无线局域网分等级实施安全保护。

3.1.5

公众无线局域网安全风险 Security Risk of Public Wireless Local Area Network

人为或自然的威胁可能利用公众无线局域网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。

3.1.6

公众无线局域网安全风险评估 security risk assessment of public wireless local area network

运用科学的方法和手段，系统地分析公众无线局域网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，提出有针对性的抵御威胁的防护对策和安全措施。防范和化解公众无线局域网安全风险，或者将风险控制在可接受的水平，为最大限度地为保障公众无线局域网的安全提供科学依据。

3.1.7

公众无线局域网资产 Asset of Public Wireless Local Area Network

公众无线局域网中具有价值的资源，是安全防护保护的对象。公众无线局域网中的资产可能是以多种形式存在，无形的、有形的、硬件、软件，包括物理布局、通信设备、物理线路、数据、软件、文档、规程、业务承载能力、人员、管理等各种类型的资源。公众无线局域网中的典型资产包括AC、AP、Radius、Web Portal等。

3.1.8

公众无线局域网威胁 Threat of Public Wireless Local Area Network

可能导致对公众无线局域网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。

3.1.9

公众无线局域网脆弱性 Vulnerability of Public Wireless Local Area Network

脆弱性是公众无线局域网中存在的弱点、缺陷与不足，不直接对公众无线局域网资产造成危害，但可能被公众无线局域网威胁所利用从而危及公众无线局域网资产的安全。

3.1.10

公众无线局域网灾难 Disaster of Public Wireless Local Area Network

由于各种原因，造成公众无线局域网故障或瘫痪，使公众无线局域网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

公众无线局域网灾难备份 Backup for Disaster Recovery of Public Wireless Local Area Network

为了公众无线局域网灾难恢复而对相关的网络要素进行备份的过程。

3.1.12

公众无线局域网灾难恢复 Disaster Recovery of Public Wireless Local Area Network

为了将公众无线局域网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

无线破解攻击 Wireless Crack Attack

攻击者使用工具，通过捕获802.11报文，采用逆向算法获得WLAN网络密钥，或者通过弱口令字典，并辅以不断尝试认证，对WLAN网络进行暴力破解，达到入侵的目的。

3.1.14**无线钓鱼攻击 Wireless Fishing Attack**

攻击者通过工具或者搭建软AP，在目标WLAN网络附近，构造与目标WLAN网络相同或者相近的网络，引诱受害者连接，一旦连接建立，攻击者会进一步截获受害者的网络流量，获取敏感信息。

3.1.15**无线中间人攻击 Wireless Man-In-The-Middle Attack**

攻击者通过伪造WLAN网络标识、MAC地址等物理信息，对特定用户的无线通信进行欺骗，使得正常的通信流量流经攻击者，攻击者可以在流量中插入攻击代码或截获流量中的敏感信息，发起进一步的攻击。

3.1.16**无线DoS攻击 Wireless Denial of Service Attack**

攻击者通过向WLAN网络中发送大量伪造的认证、关联等802.11报文，从而达到让AP或AC过载的目的，使得正常用户无法接入WLAN网络；或者通过发送大量伪造的去认证、去关联等802.11报文，拆除已经建立的WLAN连接，导致用户无法通过WLAN网络接入。

3.1.17**无线注入攻击 Wireless Injection Attack**

攻击者通过伪造802.11报文，向WLAN网络中注入流量，例如通过注入ARP Request（地址解析协议请求），对WLAN进行干扰，达到加快破解的目的；通过无线注入攻击，攻击者也可以伪造网络向量分配，抢占WLAN信道通信时间，实现拒绝服务攻击；攻击者也可以通过注入更为复杂的流量，达到网络欺骗的目的。

3.1.18**hotspotter攻击 Hotspotter Attack**

攻击者监测WLAN网络中的探测请求，并将发现的WLAN网络与自身的WLAN热点列表进行对比，如果一旦发现匹配的WLAN网络，攻击发起者会伪造认证和关联过程，引诱用户，一旦连接建立，攻击者会进一步对受害者进行毒化或扫描，并发起进一步的攻击。

3.1.19**SQL注入攻击 Sql Injection**

SQL注入是一个代码注入技术，它利用一个web应用程序的安全漏洞，在数据库层实施攻击。如果对用户输入的非法字符串（如web表单递交或输入域名或页面请求的查询字符串）过滤不严谨，则会把构建的恶意SQL语句传递到数据库，欺骗服务器执行恶意的SQL命令中执行。

3.1.20**跨站脚本攻击 Cross Site Scripting**

一种web应用程序的漏洞类型，能令攻击者插入客户端脚本到web页面，当其他用户查看时被攻击。

3.1.21

网页木马 Web-Page Trojan

表面上伪装成普通的网页文件或是将恶意的代码直接插入到正常的网页文件中，当有人访问时，网页木马就会利用对方系统或者浏览器的漏洞自动将配置好的木马的服务端下载到访问者的电脑上来自动执行。

3.1.22**TCP拒绝服务 TCP Flood**

一种拒绝服务攻击，利用TCP协议缺陷，发送大量伪造的TCP连接请求，从而使得被攻击方资源耗尽（CPU满负荷或内存不足）的攻击方式。

3.1.23**Portal 服务器 Portal Server**

Portal是一种web应用，通常用来提供个性化、单点登录、聚集各个信息源的内容，并作为信息系统表现层的宿主。聚集是指将来自各个信息源的内容集成到一个web页面里的活动。

3.2 缩略语

下列缩略语适用于本标准。

| | | |
|--------|--|--------------|
| AC | Access Point Controller | 接入控制器 |
| ACL | Access Control List | 访问控制列表 |
| AP | Access Point | 接入点 |
| BGP | Border Gateway Protocol | 边界网关协议 |
| BRAS | Broadband Remote Access Server | 宽带接入服务器 |
| DDoS | Distributed Denial of Service | 分布式拒绝服务攻击 |
| DNS | Domain Name System | 域名系统 |
| DSL | Digital Subscriber Line | 数字用户专线 |
| HA | High Availability | 高可用性 |
| HTTP | Hypertext Transfer Protocol | 超文本传输协议 |
| IP | Internet Protocol | 网际协议 |
| ISIS | Intermediate system to intermediate system | 中间系统到中间系统 |
| MAC | Media Access Control | 介质访问控制 |
| OSPF | Open Shortest Path First | 开放式最短路径优先 |
| PON | Passive Optical Network | 无源光纤网络 |
| PWLAN | Public Wireless Local Area Network | 公众无线局域网 |
| RADIUS | Remote Authentication Dial In User Service | 远程访问拨号接入用户服务 |
| SQL | Structured Query Language | 结构化查询语言 |
| SSH | Secure Shell | 安全外壳协议 |
| WIPS | Wireless Intrusion Prevention System | 无线入侵防御系统 |
| WLAN | Wireless Local Area Networks | 无线局域网 |
| XSS | Cross Site Script | 跨站脚本攻击 |

4 PWLAN 安全防护检测概述

4.1 PWLAN 安全防护检测内容

本标准的安全防护检测内容与YD/T 2696-2014《公众无线局域网安全防护要求》一致，包括业务安全、设备及软件系统安全、网络安全、物理环境安全和管理安全。

4.2 PWLAN 安全防护检测对象

PWLAN安全防护检测对象是基础电信业务经营者和增值电信业务经营者建设或者运营的公众无线局域网，本标准主要对公众无线局域网的各项要求的实施进行检测。

4.3 PWLAN 安全防护检测环境

对PWLAN的安全防护检测需在现网中进行，其检测环境结构示意图如图1所示。

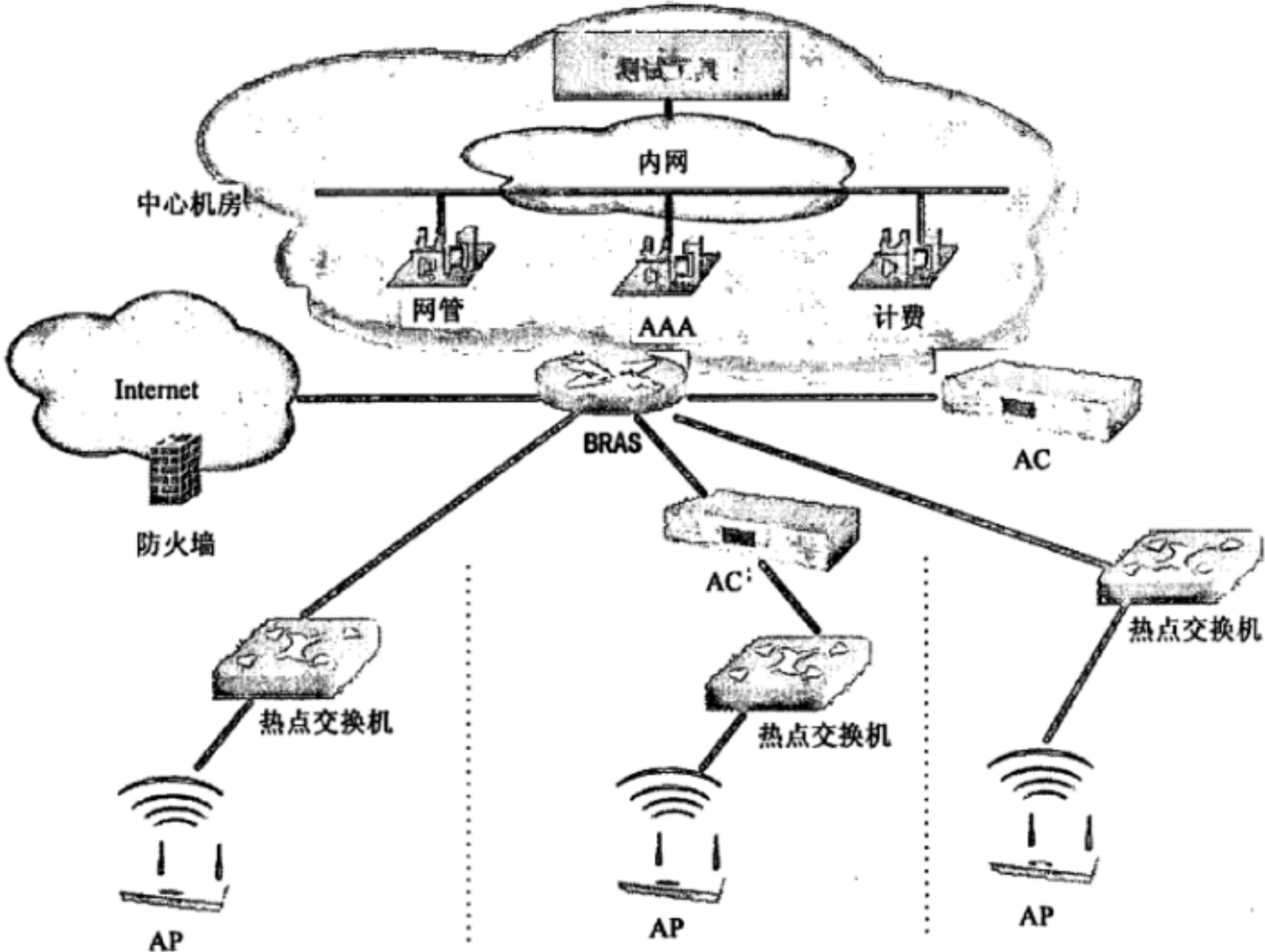


图1 PWLAN 安全防护检测环境结构示意图

被测对象包括：PWLAN网络设备（如AC、AP、BRAS、热点交换机等）和PWLAN辅助性IT系统（如运维、管理、监测系统等）。

测试工具包括：协议分析仪（应支持IP协议簇各层协议的解析）和漏洞扫描器（应支持主机扫描、端口扫描、漏洞检测等功能）。

5 PWLAN 安全防护检测要求

5.1 第1级要求

5.1.1 业务安全要求

5.1.1.1 业务认证管理

| |
|--|
| 测试编号: PWLAN-第1级-业务安全-业务认证管理-01 |
| 测试项目: 《公众无线局域网安全防护要求》5.1.1.1-a, 用户的身份标识和鉴别要求 |
| 测试步骤: 1) 创建合法测试账号, 并保证账号功能正常; 2) 使用合法测试账号, 提供正确的鉴别信息执行登录系统操作; 3) 检查系统是否通过了合法测试账户的登录操作; 4) 使用合法测试账户, 提供错误的鉴别信息执行登录系统操作; 5) 检查系统是否拒绝合法测试账户的登录操作; 6) 使用无效的测试账户, 执行登录系统操作; 7) 检查系统是否拒绝无效测试账户的登录操作 |
| 预期结果: 1) 系统对提供正确鉴别信息的合法测试账户的登录操作, 予以通过; 2) 系统对提供错误鉴别信息的合法测试账户的登录操作, 予以拒绝; 3) 系统对无效测试账户的登录操作, 予以拒绝 |
| 判定原则: 达到以上预期结果, 则通过, 否则不通过 |

| |
|--|
| 测试编号: PWLAN-第1级-业务安全-业务认证管理-02 |
| 测试项目: 《公众无线局域网安全防护要求》5.1.1.1-b, 加密方式传输用户的口令信息 |
| 测试步骤: 1) 访谈相关技术人员, 确认系统设计, 传输业务用户的密码信息时是否进行了加密; 2) 通过抓包等方式, 截获数据; 3) 验证是否以加密方式传输用户的口令信息 |
| 预期结果: 1) 系统设计中, 传输业务用户的密码信息, 需进行加密; 2) 抓包结果分析显示采用密文方式传输用户的口令信息 |
| 判定原则: 达到以上预期结果, 则通过, 否则不通过 |

| |
|---|
| 测试编号: PWLAN-第 1 级-业务安全-业务认证管理-03 |
| 测试项目: 《公众无线局域网安全防护要求》5.1.1.1-c, 加密方式存储用户的口令信息 |
| 测试步骤: 1) 访谈相关技术人员, 确认系统设计, 存储业务用户的密码信息时是否进行了加密; 2) 查看业务用户密码信息, 验证系统是否存在明文方式存储的业务用户的密码信息; 3) 创建测试账户, 查看测试账户的密码信息, 是否以密文方式存储 |
| 预期结果: 1) 系统设计中, 存储业务用户的密码信息, 需进行加密; 2) 系统中当前的存储中, 不存在明文形式的用户密码信息; 3) 系统存储新建测试账户的密码信息时, 采用密文方式存储 |
| 判定原则: 达到以上预期结果, 则通过, 否则不通过 |

5.1.1.2 业务资源控制

| |
|---|
| 测试编号: PWLAN-第 1 级-业务安全-业务资源控制-01 |
| 测试项目: 《公众无线局域网安全防护要求》5.1.1.2-a, 用户异常掉线后, AC、AP 应释放内存、回收资源 |
| 测试步骤: 1) 使用测试客户端与 AP 连接; 2) 检验连接是否正常; 3) 查看 AC 和 AP 的关联表, 是否新增连接信息; 4) 采用异常方式断开无线客户端与 AP 的连接, 使得无线客户端掉线; 5) 查看 AC 和 AP 的关联表, 查看系统是否更新连接信息, 能否自动释放内存、回收资源 |
| 预期结果: 1) 测试客户端与 AP 正常连接, AC 和 AP 关联表显示成功分配资源; 2) 断开测试客户端与 AP 的连接之后, AC 和 AP 关联表上无该客户端的正在连接 AP 的信息 |
| 判定原则: 达到以上预期结果, 则通过, 否则不通过 |

5.1.1.3 业务安全防范

| |
|--|
| 测试编号: PWLAN-第 1 级-业务安全-业务安全防范-01 |
| 测试项目: 《公众无线局域网安全防护要求》5.1.1.3-a, 应具备发现和处理含有恶意代码链接的能力 |
| 测试步骤: 1) 询问技术人员针对恶意代码链接采取了何种安全防护措施; 2) 网页扫描检查 PWLAN 登录页面是否存在恶意代码链接; 3) 构造恶意代码链接; 4) 验证是否可以在 PWLAN 登录页面嵌入恶意代码链接 |
| 预期结果: 1) 网页扫描检查未发现已嵌入的恶意代码链接; 2) 无法进行恶意代码链接渗透攻击 |
| 判定原则: 达到以上预期结果, 则通过, 否则不通过。 |

| |
|---|
| 测试编号: PWLAN-第 1 级-业务安全-业务安全防范-02 |
| 测试项目: 《公众无线局域网安全防护要求》5.1.1.3-b, 应具备防护 SQL 注入攻击和变种注入攻击的能力 |
| 测试步骤: 1) 询问技术人员采取了何种措施防护 SQL 注入攻击和变种注入攻击; 2) 构造 SQL 注入语句, 验证 Portal 页面和 PWLAN 设备管理页面是否存在可被利用的 SQL 注入漏洞; 3) 构造 SQL 注入语句, 验证 AP、AC、热点交换机的 Web 管理页面是否存在可被利用的 SQL 注入漏洞 |
| 预期结果: 1) Portal 页面和 PWLAN 设备管理页面不存在注入漏洞; 2) AP、AC、热点交换机的 Web 管理页面不存在可被利用的 SQL 注入漏洞 |
| 判定原则: 达到以上预期结果, 则通过, 否则不通过 |

| |
|---|
| 测试编号: PWLAN-第 1 级-业务安全-业务安全防范-03 |
| 测试项目: 《公众无线局域网安全防护要求》5.1.1.3-c, 应具备 URL 访问控制能力 |
| 测试步骤: 1) 询问技术人员采取了何种 URL 访问控制措施; 2) 创建测试账号; 3) 使用测试账号登录系统; 4) 记录登录后的 URL 地址; 5) 测试账号退出系统; 6) 构造特定的 URL, 输入 4) 中记录的 URL 地址, 查看是否可以利用修改 URL 参数的方式绕过认证 |
| 预期结果: 1) 测试账号正常登陆; 2) 无法利用特定的 URL 访问未经认证后的页面。 |
| 判定原则: 达到以上预期结果, 则通过, 否则不通过 |

5.1.1.4 业务安全审计

| |
|--|
| 测试编号: PWLAN-第 1 级-业务安全-业务安全审计-01 |
| 测试项目: 《公众无线局域网安全防护要求》5.1.1.4-a, 审计范围应覆盖到每个用户的关键操作、重要行为、业务资源使用情况等重要事件 |
| 测试步骤: 1) 检查业务设计/验收文档, 确认系统的审计范围是否覆盖到每个用户的关键操作、重要行为、业务资源使用情况等重要事件, 如普通用户异常登录、发布恶意代码、异常修改账号信息等行为, 以及管理员在业务功能及账号控制方面的关键操作; 2) 打开系统审计记录; 3) 检查审计范围是否覆盖到每个用户的关键操作、重要行为、业务资源使用情况等重要事件 |
| 预期结果: 1) 审计记录在设计时, 包括了每个用户的关键操作、重要行为、业务资源使用情况等重要事件, 包括如普通用户异常登录、发布恶意代码、异常修改账号信息等行为, 以及管理员在业务功能及账号控制方面的关键操作; 2) 现存的系统审计记录范围覆盖到了每个用户的关键操作、重要行为、业务资源使用情况等重要事件 |
| 判定原则: 达到以上预期结果, 则通过, 否则不通过 |

| |
|--|
| 测试编号: PWLAN-第1级-业务安全-业务安全审计-02 |
| 测试项目: 《公众无线局域网安全防护要求》5.1.1.4-b, 应保护审计记录, 保证无法删除、修改或覆盖等 |
| 测试步骤: 1) 登录审计系统; 2) 尝试删除一条或多条审计信息; 3) 尝试修改一条或多条审计信息; 4) 尝试覆盖一条或多条审计信息; 5) 询问技术人员审计信息存储的周期、方式等 |
| 预期结果: 1) 审计信息不能被删除; 2) 审计信息不能被修改; 3) 审计信息不能被覆盖 |
| 判定原则: 达到以上预期结果, 则通过, 否则不通过 |

| |
|---|
| 测试编号: PWLAN-第1级-业务安全-业务安全审计-03 |
| 测试项目: 《公众无线局域网安全防护要求》5.1.1.3-c, 业务相关审计记录应包括事件日期、时间、发起者信息、类型、描述和结果等 |
| 测试步骤: 1) 检查业务设计/验收文档, 确认系统的审计记录是否包括事件日期、时间、发起者信息、类型、描述和结果等类型; 2) 打开业务相关审计记录; 3) 检查实际记录中是否包括事件日期、时间、发起者信息、类型、描述和结果等 |
| 预期结果: 1) 审计记录在设计时, 包括事件日期、时间、发起者信息、类型、描述和结果等类型; 2) 实际的业务相关审计记录包括了事件日期、时间、发起者信息、类型、描述和结果等 |
| 判定原则: 达到以上预期结果, 则通过, 否则不通过 |

5.1.2 设备及软件系统安全要求

5.1.2.1 AC、AP 及热点交换机设备

| |
|--|
| 测试编号: PWLAN-第 1 级-设备及软件系统安全要求-AC、AP 及热点交换机设备-01 |
| 测试项目: 《公众无线局域网安全防护要求》5.1.2.1-a, AC 设备在应用层应对 Cookies 或者 Session 做判断 |
| 测试步骤: 1) 询问技术人员对 AC 设备采取了何种防护措施; 2) 使用漏洞扫描工具对 AC 进行扫描; 3) 检测设备是否存在应用层漏洞; 4) 扫描设备是否开启不必要端口; 5) 尝试能否破解管理员密码 |
| 预期结果: 1) AC 设备不存在应用层漏洞; 2) 无多余端口打开; 3) 无法破解管理员密码 |
| 判定原则: 达到以上预期结果, 则通过, 否则不通过 |

| |
|---|
| 测试编号: PWLAN-第 1 级-设备及软件系统安全要求-AC、AP 及热点交换机设备-02 |
| 测试项目: 《公众无线局域网安全防护要求》5.1.2.1-b, AC、Radius 设备应支持 SSH、HTTPS 等加密形式登陆 |
| 测试步骤: 1) 询问技术人员对 AC、Radius 设备采取了何种防护措施; 2) 创建测试账号, 并保证账号功能正常; 3) 登录 AC、Radius 服务器; 4) 通过抓包等方式, 截获数据; 5) 验证数据中是否存在明文设备管理密码; 6) 查看是否采用 SSH 或 HTTPS 等加密的登录方式; 7) 检查 AC、Radius 服务器是否关闭了 Telnet 等未加密的管理服务 |
| 预期结果: 1) 测试账号正常登录; 2) 网络中没有发现明文的用户密码; 3) 采用了 SSH 或 HTTPS 等加密技术确保用户密码的传输安全; 4) AC、Radius 服务器关闭了未加密管理方式 |
| 判定原则: 达到以上预期结果, 则通过, 否则不通过 |

| |
|--|
| 测试编号: PWLAN-第1级-设备及软件系统安全要求-AC、AP及热点交换机设备-03 |
| 测试项目: 《公众无线局域网安全防护要求》5.1.2.1-c, AC设备应开启防护功能 |
| 测试步骤: 1) 登录AC设备, 检查AC配置; 2) 查看是否开启端口隔离; 3) 查看是否开启用户隔离; 4) 查看是否开启非法AP检测功能 |
| 预期结果: 1) 登录AC设备成功; 2) AC设备开启了端口隔离; 3) AC设备开启了用户隔离; 4) AC设备开启了非法AP检测 |
| 判定原则: 达到以上预期结果, 则通过, 否则不通过 |

| |
|--|
| 测试编号: PWLAN-第1级-设备及软件系统安全要求-AC、AP及热点交换机设备-04 |
| 测试项目: 《公众无线局域网安全防护要求》5.1.2.1-d, AP设备和热点交换机应开启二层隔离功能 |
| 测试步骤: 1) 登录AP设备和热点交换机; 2) 检查AP和热点交换机的配置; 3) 查看是否开启了二层隔离 |
| 预期结果: 1) 登录AP设备和热点交换机成功; 2) AP和交换机开启二层隔离 |
| 判定原则: 达到以上预期结果, 则通过, 否则不通过 |

| |
|---|
| 测试编号: PWLAN-第1级-设备及软件系统安全要求-AC、AP及热点交换机设备-05 |
| 测试项目: 《公众无线局域网安全防护要求》5.1.2.1-f, AC设备上应配置ACL |
| 测试步骤: 1) 登录AC设备和防火墙; 2) 查看AC和防火墙上是否配置了访问控制策略; 3) 确保DNS端口号53的UDP报文只允许访问DNS服务器 |
| 预期结果: 1) 登录AC设备和防火墙成功; 2) AC上配置了访问控制策略, 无法进行DNS Tunnel 绕过 |
| 判定原则: 达到以上预期结果, 则通过, 否则不通过 |

5.1.2.2 网络设备

| |
|--|
| 测试编号: PWLAN-第1级-设备及软件系统安全要求-网络设备-01 |
| 测试项目: 《公众无线局域网安全防护要求》5.1.2.2-a, PWLAN相关网络设备应满足YD/T 2698-2014《电信网与互联网安全防护基线配置要求及检测要求 网络设备》的安全要求 |
| 测试步骤: 1) 访谈设备采购管理、运维和安全管理人員, 查看设备入网检测报告、安全检测报告等; 2) 检查PWLAN网络中的路由器、交换机、AC、AP等设备是否符合YD/T 2698-2014《电信网与互联网安全防护基线配置要求及检测要求 网络设备》要求 |
| 预期结果: PWLAN现网使用的网络设备符合YD/T 2698-2014《电信网与互联网安全防护基线配置要求及检测要求 网络设备》要求 |
| 判定原则: 达到以上预期结果, 则通过, 否则不通过 |

5.1.2.3 数据库

| |
|--|
| 测试编号: PWLAN-第1级-设备及软件系统安全要求-数据库-01 |
| 测试项目: 《公众无线局域网安全防护要求》5.1.2.3-a, 数据库的安全应满足 YD/T 2700-2014《电信网与互联网安全防护基线配置要求及检测要求 数据库》的安全要求 |
| 测试步骤: 1) 访谈运维和安全管理人員, 查看数据库安全检测报告等; 2) 检查PWLAN网络中数据库系统是否符合YD/T 2700-2014《电信网与互联网安全防护基线配置要求及检测要求 数据库》要求 |
| 预期结果: PWLAN 使用的数据库符合 YD/T 2700-2014《电信网与互联网安全防护基线配置要求及检测要求 数据库》要求 |
| 判定原则: 达到以上预期结果, 则通过, 否则不通过 |

5.1.2.4 操作系统

| |
|--|
| 测试编号: PWLAN-第1级-设备及软件系统安全要求-操作系统-01 |
| 测试项目: 《公众无线局域网安全防护要求》5.1.2.4-a, 操作系统的安全应满足 YD/T 2701-2014《电信网与互联网安全防护基线配置要求及检测要求 操作系统》的安全要求 |
| 测试步骤: 1) 访谈运维和安全管理人員, 查看操作系统安全检测报告等; 2) 检查PWLAN网络中的操作系统是否满足YD/T 2701-2014《电信网与互联网安全防护基线配置要求及检测要求 操作系统》要求 |
| 预期结果: PWLAN 使用的操作系统符合 YD/T 2701-2014《电信网与互联网安全防护基线配置要求及检测要求 操作系统》要求 |
| 判定原则: 达到以上预期结果, 则通过, 否则不通过 |

5.1.3 网络安全要求

5.1.3.1 网络拓扑

| |
|--|
| 测试编号: PWLAN-第1级-网络安全要求-网络拓扑-01 |
| 测试项目: 《公众无线局域网安全防护要求》5.1.3.1-a, PWLAN 节点部署合理, 具有较高的可用性和可扩展性 |
| 测试步骤: 1) 访谈 PWLAN 运维人员, 查看网络节点部署规划和路由使用情况; 2) 检查并核对网络设备实际部署和配置情况; 3) 核对网络及设备实际配置信息; 4) 在网络节点接口处使用协议分析仪对路由报文进行抓取和分析; 5) 评估 PWLAN 网络是否具有较高的可用性和可扩展性 |
| 预期结果: 1) PWLAN 节点部署及路由的部署合理; 2) 网络设备配置信息无错误; 3) 网络拓扑具有可扩展性; 4) PWLAN 网络节点接口使用的路由协议均具有较高的可用性和可扩展性 |
| 判定原则: 达到以上预期结果, 则通过, 否则不通过 |

5.1.3.2 网络保护与恢复

| |
|---|
| 测试编号: PWLAN-第1级-网络安全要求-网络保护与恢复-01 |
| 测试项目: 《公众无线局域网安全防护要求》5.1.3.2-a, PWLAN 节点重要部件和模块应配置为主备用方式 |
| 测试步骤: 1) 访谈网络运维人员; 2) 查看网络设备配置文档、故障告警记录等; 3) 检查AC、Radius服务器等重要节点的电源或主控是否为主备用方式; 4) 在业务空闲时段对PWLAN节点设备重要部件进行主备切换, 验证其是否采用主备冗余保护措施 |
| 预期结果: 1) 配置文档、故障记录记录完整; 2) AC、Radius 服务器等设备电源模块采用了主备冗余保护措施; 3) AC、Radius 服务器等设备主控模块采用了主备冗余保护措施 |
| 判定原则: 达到以上预期结果, 则通过, 否则不通过 |

| |
|--|
| 测试编号: PWLAN-第1级-网络安全要求-网络保护与恢复-02 |
| 测试项目:《公众无线局域网安全防护要求》5.1.3.2-b, PWLAN 重要节点(如 AC、BRAS 等)间链路应采取链路冗余保护措施 |
| 测试步骤: 1) 访谈网络运维人员; 2) 查看网络设计、设备配置文档、故障告警记录等; 3) 检查重要节点间链路冗余配置和使用情况; 4) 在业务空闲时段对 PWLAN 重要节点间单条链路进行切断和恢复操作,验证 PWLAN 网络链路的容灾抗灾能力 |
| 预期结果: 1) 网络设计、配置文档、故障记录完好,网络重要节点间链路有冗余链路相关设计且与实施部署相一致; 2) 网络切换可正常使用,冗余生效; 3) 冗余链路等方式能够满足 PWLAN 网络链路的容灾抗灾要求; 4) 冗余链路等方式保护的灾难恢复时间能够满足预先设定的目标 |
| 判定原则: 达到以上预期结果,则通过,否则不通过 |

| |
|---|
| 测试编号: PWLAN-第1级-网络安全要求-网络保护与恢复-03 |
| 测试项目:《公众无线局域网安全防护要求》5.1.3.2-c, PWLAN 应根据应用的需求采用链路聚合、保护倒换等安全保护措施 |
| 测试步骤: 1) 访谈 PWLAN 运维人员; 2) 查看网络设计文档、设备配置记录、运行历史记录、故障告警记录等; 3) 检查 PWLAN 链路部署情况和重要设备配置信息; 4) 检查 PWLAN 根据业务或应用的需求所采用链路聚合、转发检测、保护倒换、重路由等安全保护措施的情况 |
| 预期结果: 1) 网络设计文档、设备配置信息合理; 2) 运行记录、故障记录完好; 3) PWLAN 网络中根据需要设置了链路聚合、转发检测、保护倒换、重路由等措施,并生效; 4) PWLAN 网络采用的上述安全保护措施能够满足业务或应用的需要 |
| 判定原则: 达到以上预期结果,则通过,否则不通过 |

5.1.3.3 网络管理

| |
|---|
| 测试编号: PWLAN-第1级-网络安全要求-网络管理-01 |
| 测试项目: 《公众无线局域网安全防护要求》5.1.3.3-a, PWLAN 应根据网络结构形式采用分域的管理方式 |
| 测试步骤: 1) 访谈网络运维和安全管理人員; 2) 查看网络拓扑文档、网络管理规章、设备管理记录等; 3) 检查网络管理是否采用分域的管理方式; 4) 检查网络是否根据实际需求或运维体制设置分级权限, 对网络设备和运维人员进行分级管理; 5) 管理员进行权限内操作; 6) 管理员尝试进行非权限内操作 |
| 预期结果: 1) 文档记录合理完好; 2) PWLAN 根据网络结构特点, 采用分域的管理方式; 3) 网络管理根据实际需求或运维体制设置分级权限; 4) 管理员可以在权限内操作; 5) 管理员在非权限内不可操作 |
| 判定原则: 达到以上预期结果, 则通过, 否则不通过 |

| |
|--|
| 测试编号: PWLAN-第1级-网络安全要求-网络管理-02 |
| 测试项目: 《公众无线局域网安全防护要求》5.1.3.3-b, PWLAN 业务网络与运维、管理、监测等辅助系统(或平台)间应实现逻辑隔离 |
| 测试步骤: 1) 访谈网络运维和安全管理人員, 查看网络设计文档、网络安全策略、运维管理制度、设备配置文档等; 2) 检查网络、设备的配置以及相关辅助系统的连接和组网情况; 3) 从 PWLAN 业务网络侧访问辅助系统中的设备, 验证网络与辅助系统间是否实现逻辑隔离, 评估安全域访问控制策略的应用效果; 4) 使用网络维护终端访问辅助系统中的设备, 验证是否有安全的访问认证措施对其进行限制 |
| 预期结果: 1) 网络规划合理, 文档完整; 2) PWLAN 运维、管理、监测等辅助系统(或平台)与业务网络间采用了逻辑隔离的隔离措施, 违反安全策略的访问被限制; 3) 网络维护终端访问被管理网络设备时采取了安全措施, 违反安全策略的访问被限制 |
| 判定原则: 达到以上预期结果, 则通过, 否则不通过 |

| |
|--|
| 测试编号: PWLAN-第1级-网络安全要求-网络管理-03 |
| 测试项目: 《公众无线局域网安全防护要求》5.1.3.3-c, PWLAN 网络管理应使用用户安全鉴别和认证措施 |
| 测试步骤: 1) 访谈网络运维和安全管理人員, 查看网络运维管理规章、网络安全策略、设备配置文档等, 查看PWLAN 网络管理针对用户认证的要求; 2) 检查网络管理设备是否采用了用户安全鉴别和认证措施, 用户登录口令是否符合要求; 3) 构造特殊用户名尝试登录网络管理设备 |
| 预期结果: 网络管理使用了用户安全鉴别和认证措施 |
| 判定原则: 达到以上预期结果, 则通过, 否则不通过 |

| |
|--|
| 测试编号: PWLAN-第1级-网络安全要求-网络管理-04 |
| 测试项目: 《公众无线局域网安全防护要求》5.1.3.3-d, PWLAN 应有与当前网络节点、链路、频谱等资源配置和运营情况相符合的网络拓扑图 (或记录完整拓扑信息的运维文档) |
| 测试步骤: 1) 访谈网络运维和安全管理人員; 2) 查看网络拓扑文档; 3) 检查网络拓扑记录信息是否与当前网络节点、链路等资源配置和运营情况相一致 |
| 预期结果: 1) 绘制有网络拓扑图 (或记录完整拓扑信息的运维文档), 且相关信息标注完整、准确; 2) 网络拓扑图 (或记录完整拓扑信息的运维文档) 及相关信息与当前网络节点、链路等资源配置和运营情况相符合 |
| 判定原则: 达到以上预期结果, 则通过, 否则不通过 |

| |
|--|
| 测试编号: PWLAN-第 1 级-网络安全要求-网络管理-05 |
| 测试项目: 《公众无线局域网安全防护要求》5.1.3.3-e, PWLAN 的网络管理应启用访问和资源控制的安全措施 |
| 测试步骤: 1) 访谈网络运维和安全管理人員, 查看网络安全策略、设备配置记录、账号权限管理和分配记录、日志记录等; 2) 检查PWLAN网络设备是否启用访问和资源控制的安全配置; 3) 通过网络渗透工具对被测网络进行渗透测试 |
| 预期结果: 1) PWLAN 网络管理和维护操作涉及的相关设备资源访问、调用等均使用了严格的访问控制策略及保护措施; 2) PWLAN 的业务控制与管理相关用户的账号权限均依据最小授权原则(即授予特定账号为完成其承担任务所需的最小权限)进行管; 3) PWLAN 相关设备均禁用了默认账号(或严格限制默认账号权限) |
| 判定原则: 达到以上预期结果, 则通过, 否则不通过 |

| |
|--|
| 测试编号: PWLAN-第 1 级-网络安全要求-网络管理-06 |
| 测试项目: 《公众无线局域网安全防护要求》5.1.3.3-f, PWLAN 管理信息及数据的机密性和完整性在传送、接收、处理和存储过程中都应得到保证 |
| 测试步骤: 1) 访谈网络运维和安全管理人員, 查看网络管理系统设计文档、网络安全策略、设备配置记录、日志和审计记录、数据存储和使用记录等, 查看网络管理数据是否满足完整性和机密性; 2) 检查网络管理时采用的安全设备及采用的通信协议; 3) 使用协议分析仪对网络管理数据报文进行抓包, 分析报文的完整性和机密性; 4) 检查存储于管理系统中的相关管理数据的完整性和机密性 |
| 预期结果: 1) PWLAN 具有管理信息及数据机密性和完整性保护设计, 实际采用了数据信息机密性和完整性保护措施; 2) PWLAN 的管理信息及数据的机密性和完整性在传送、接收、处理和存储过程中都能得到保证 |
| 判定原则: 达到以上预期结果, 则通过, 否则不通过 |

5.1.3.4 网络安全监测

| |
|--|
| 测试编号: PWLAN-第1级-网络安全要求-网络安全监测-01 |
| 测试项目: 《公众无线局域网安全防护要求》5.1.3.4-a, 应具备关键设备 (AC、Radius) 和数据库运行状态监测功能 |
| 测试步骤: 1) 访谈技术人员是否具备关键设备 (AC、Radius) 和数据库运行状态监测功能; 2) 查看监测信息是否包括PWLAN设备网络运行状态、CPU和内存, 并与实际情况对比; 3) 查看监测信息是否包括在线用户数量、信道使用情况; 4) 查看监测信息是否包括数据库的版本信息、表空间利用率和数据库表操作记录 |
| 预期结果: 1) 监测到的网络运行状态/CPU/内存等信息与实际相符; 2) 监测信息包括用户数量/信道使用情况等; 3) 监测信息包括数据库版本信息、表空间利用率和数据库表操作记录 |
| 判定原则: 达到以上预期结果, 则通过, 否则不通过 |

| |
|---|
| 测试编号: PWLAN-网络安全要求-网络安全监测-02 |
| 测试项目: 《公众无线局域网安全防护要求》5.1.3.4-b, 应具备安全告警事件监测功能 |
| 测试步骤: 1) 访谈技术人员是否具备安全告警事件监测功能; 2) 查看网络设备及认证系统产生的告警日志; 3) 触发告警信息, 查看安全事件告警上报是否实时; 4) 查看安全事件的处理情况 |
| 预期结果: 1) 存有网络设备和认证系统产生的告警日志; 2) 告警信息可以实时上报; 3) 安全事件可以及时处理 |
| 判定原则: 达到以上预期结果, 则通过, 否则不通过 |

5.1.3.5 网络安全防范

| |
|---|
| 测试编号: PWLAN-第1级-网络安全要求-网络安全防范-01 |
| 测试项目: 《公众无线局域网安全防护要求》5.1.3.5-a, PWLAN 应具有防范常见网络攻击、差错防范和处理的能力 |
| 测试步骤: 1) 访谈 PWLAN 维护和管理人员, 查看网络设计文档、网络安全策略、设备配置记录、故障告警记录、日志文件资料等, 查看 PWLAN 的网络攻击监控措施; 2) 检查 PWLAN 网络和辅助系统的配置信息, 判断其是否具有监测常见网络攻击、差错防范和处理的设计; 3) 对 AC、热点交换机等网络设备和 radius 服务器等 IT 系统进行端口扫描和网络嗅探 |
| 预期结果: 1) PWLAN 具有监测常见网络攻击、差错防范和处理的设计; 2) 网络和设备相关监测常见攻击、差错防范和处理的措施均正常启用; 3) 相关安全技术措施能够监测并抵御针对网络设备和 IT 系统的常见攻击及入侵 |
| 判定原则: 达到以上预期结果, 则通过, 否则不通过 |

| |
|--|
| 测试编号: PWLAN-第1级-网络安全要求-网络安全防范-02 |
| 测试项目: 《公众无线局域网安全防护要求》5.1.3.5-b, 应防止远程入侵计费系统 |
| 测试步骤: 1) 询问技术人员计费系统是否采取了安全防护措施; 2) 扫描工具检查计费系统是否存在安全防护; 3) 渗透技术检查计费系统是否存在安全防护; 4) 软件和配置检查系统是否存在安全防护 |
| 预期结果: 1) 扫描工具检查计费系统存在安全防护; 2) 渗透技术检查计费系统存在安全防护; 3) 软件和配置检查计费系统存在安全防护 |
| 判定原则: 达到以上预期结果, 则通过, 否则不通过 |

| |
|--|
| 测试编号: PWLAN-第1级-网络安全要求-网络安全防范-03 |
| 测试项目: 《公众无线局域网安全防护要求》5.1.3.5-c, PWLAN 应具有防范通过空口进行的网络入侵行为的能力 |
| 测试步骤: 1) 询问技术人员采用了何种防护措施防范通过空口进行的网络入侵行为; 2) 查看无线安全防护设备告警信息, 是否包括对网络入侵行为的告警 |
| 预期结果: 1) 采用了无线安全防护措施; 2) 无线安全防护设备可以上报逆向、暴力破解的告警 |
| 判定原则: 达到以上预期结果, 则通过, 否则不通过 |

| |
|--|
| 测试编号: PWLAN-第1级-网络安全要求-网络安全防范-04 |
| 测试项目: 《公众无线局域网安全防护要求》5.1.3.5-d, PWLAN 应具有防范通过空口进行的网络欺骗行为的能力 |
| 测试步骤: 1) 询问技术人员采用了何种防护措施防范通过空口进行的网络欺骗行为; 2) 设置非法 AP (AC 或安全防护设备白名单之外的 AP) 进行接入内部网络; 3) 设置合法客户端 (安全防护设备白名单中的客户端) 接入内部无线网络; 4) 设置非法客户端 (安全防护设备白名单之外客户端) 接入无线网络; 5) 设置钓鱼 AP (SSID 和内网一样, 但不属于安全防护设备的白名单) 接入内部网络; 6) 使用内部无线终端接入钓鱼 AP |
| 预期结果: 1) 非法 AP 被识别为流氓 AP; 2) 合法客户端不能连接非法 AP; 3) 非法客户端接入网络失败; 4) 上报钓鱼 AP 告警信息; 5) 内部无线终端不能接入钓鱼 AP, 钓鱼失败 |
| 判定原则: 达到以上预期结果, 则通过, 否则不通过 |

| |
|---|
| 测试编号: PWLAN-第1级-网络安全要求-网络安全防范-05 |
| 测试项目:《公众无线局域网安全防护要求》5.1.3.5-e, PWLAN应具备防范常见的应用层攻击的能力 |
| 测试步骤: 1) 询问技术人员采用了何种防护措施防范常见的应用层攻击; 2) 在监测平台查看历史记录, 查看其是否能够对应用层攻击进行监测 |
| 预期结果: 1) PWLAN具备防范常见应用层攻击的设计; 2) 相关安全技术措施能够监测并抵御针对PWLAN的应用层攻击 |
| 判定原则: 达到以上预期结果, 则通过, 否则不通过 |

| |
|--|
| 测试编号: PWLAN-第1级-网络安全要求-网络安全防范-06 |
| 测试项目:《公众无线局域网安全防护要求》5.1.3.5-f, PWLAN相关设备、系统对各类管理和维护用户应启用登录失败保护和处理措施 |
| 测试步骤: 1) 询问技术人员对各类管理和维护用户采用了何种登录失败保护和处理措施; 2) 尝试使用管理账户以错误的密码多次登录AC、Radius服务器等设备; 3) 查看是否影响设备正常工作; 4) 查看PWLAN用户能否正常接入 |
| 预期结果: 1) AC/Radius服务器等密码输入次数过多登录界面被锁; 2) 设备可正常使用; 3) 不影响PWLAN用户接入 |
| 判定原则: 达到以上预期结果, 则通过, 否则不通过 |

| |
|---|
| 测试编号: PWLAN-第1级-网络安全要求-网络安全防范-07 |
| 测试项目: 《公众无线局域网安全防护要求》5.1.3.5-g, 网络设备的软件应具备实时操作、信息处理、更新升级、差错防护、故障定位等功能 |
| 测试步骤: 1) 访谈网络运维人员, 查看网络设计文档、网络设备测试报告、设备配置记录、故障告警记录、日志文件资料等, 查看网络设备软件的维护功能; 2) 查看网络设备的配置信息和日志, 检查设备软件的信息处理、更新升级、差错防护、故障定位等功能 |
| 预期结果: 1) 网络设计文档、测试报告、配置记录、日志文件等完好; 2) 网络设备软件具备实时操作、信息更新、升级、差错防护和故障定位等功能, 并已经开启相关功能 |
| 判定原则: 达到以上预期结果, 则通过, 否则不通过 |

| |
|--|
| 测试编号: PWLAN-第1级-网络安全要求-网络安全防范-08 |
| 测试项目: 《公众无线局域网安全防护要求》5.1.3.5-h, PWLAN 建立具有介质存取、验证和转储制度, 确保备份数据授权访问 |
| 测试步骤: 1) 访谈网络运维和安全管理人員, 查看网络运维规章、介质使用记录、日志和审计文件资料等; 2) 检查是否建立介质存取、验证和转储制度并有效实施; 3) 检查介质使用、数据备份和访问等授权和管理的情况 |
| 预期结果: 1) PWLAN 数据支持介质存储/转存/备份; 2) 网络安全管理有按介质特性对灾难备份及恢复相关数据定期进行验证的制度; 3) 按介质特性对灾难备份及恢复相关数据定期进行有效性验证; 4) 有按介质特性对灾难备份及恢复相关数据定期进行有效性验证的记录或报告 |
| 判定原则: 达到以上预期结果, 则通过, 否则不通过 |

| |
|--|
| 测试编号: PWLAN-第 1 级-网络安全要求-网络安全防范-09 |
| 测试项目: 《公众无线局域网安全防护要求》5.1.3.5-i, 应至少区分并设置 PWLAN 不同功能区域, 并防止跨域访问 |
| 测试步骤: 1) 询问技术人员并查看 PWLAN 网络中是否区分设置了网络管理域、设备管理域、用户接入域等不同功能区域; 2) 检查是否采用二层、三层或防火墙等技术进行隔离; 3) 检查是否采用控制跨域访问 |
| 预期结果: 1) PWLAN 网络区分设置了网络管理域、设备管理域、用户接入域等不同功能区域; 2) 采用了二层、三层或防火墙等技术进行隔离; 3) 采用了控制跨域访问, 能够防止域用户未授权访问网络资源 |
| 判定原则: 达到以上预期结果, 则通过, 否则不通过 |

5.1.4 物理环境安全要求

| |
|--|
| 测试编号: PWLAN-第 1 级-物理环境安全要求-01 |
| 测试项目: 《公众无线局域网安全防护要求》5.1.4 -a, 应满足 YD/T 1754-2008 《电信网和互联网物理环境安全等级保护要求》中第 1 级的相关要求 |
| 测试步骤: 按照 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》中第 1 级的相关要求进行检测 |
| 预期结果: 满足 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》中第 1 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 |

| |
|--|
| 测试编号: PWLAN-第 1 级-物理环境安全要求-02 |
| 测试项目: 《公众无线局域网安全防护要求》5.1.4 -b, AP 设备应防止盗用、替换, 室外 AP 设备应具备防雨、雪、风砂、雷击等防护措施 |
| 测试步骤: 1) 查看 AP 设备放置和安装情况; 2) 检查 AP 是否能保证防止盗用、替换; 3) 检查室外 AP 设备是否具备防雨、雪、风砂、雷击等相关措施 |
| 预期结果: 1) AP 设备符合防止盗用、替换等要求; 2) 室外 AP 设备具备防雨、雪、风砂、雷击等要求 |
| 判定原则: 达到以上预期结果, 则通过, 否则不通过 |

5.1.5 管理安全要求

| |
|---|
| 测试编号: PWLAN-第 1 级-管理安全要求-01 |
| 测试项目: 《公众无线局域网安全防护要求》5.1.5 -a, 满足 YD/T 1756-2008 《电信网和互联网管理安全等级保护要求》中第 1 级的相关要求 |
| 测试步骤: 按照 YD/T 1757-2008 《电信网和互联网管理安全等级保护检测要求》中第 1 级的相关要求进行检测 |
| 预期结果: 满足 YD/T 1757-2008 《电信网和互联网管理安全等级保护检测要求》中第 1 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 |

| |
|--|
| 测试编号: PWLAN-第1级-管理安全要求-02 |
| 测试项目:《公众无线局域网安全防护要求》5.1.5 -b, 安全风险评估至少应覆盖相关技术风险和管理风险, 至少包含必要要素和内容, 并根据评估结果制定相应的风险处理计划 |
| 测试步骤: 1) 访谈网络安全管理人员, 查看风险评估报告、风险处理计划和报告、安全加固和升级记录等; 2) 检查PWLAN安全风险评估是否覆盖业务安全、应用系统安全、设备安全、网络安全、物理环境安全等相关技术风险和人员安全、运维安全等相关管理风险; 3) 检查风险评估要素是否包含了资产、脆弱性、威胁、安全措施、风险和残余风险等要素, 且是否同时包含了与这些要素密切相关的属性, 如业务、资产价值、安全需求和安全事件等; 4) 检查是否根据评估结果制定相应的风险处理计划 |
| 预期结果: 1) 风险评估报告完好; 1) PWLAN 网络安全风险评估覆盖完全; 2) 具有相应的风险处理计划 |
| 判定原则: 达到以上预期结果, 则通过, 否则不通过 |

| |
|--|
| 测试编号: PWLAN-第1级-管理安全要求-03 |
| 测试项目:《公众无线局域网安全防护要求》5.1.5 -c, PWLAN 应按照 YD/T 1731-2008《电信网和互联网灾难备份及恢复实施指南》的相关要求制定灾难恢复预案 |
| 测试步骤: 1) 访谈网络安全管理人员; 2) 查看网络灾难恢复预案、预案教育培训和演练记录等; 3) 检查PWLAN灾难恢复预案是否符合YD/T 1731-2008《电信网和互联网灾难备份及恢复实施指南》的相关要求; 4) 检查灾难恢复预案的教育、培训、演练周期是否符合要求 |
| 预期结果: 1) 网络灾难恢复预案、预案教育培训和演练记录完好; 2) PWLAN 灾难恢复预案符合 YD/T 1731-2008《电信网和互联网灾难备份及恢复实施指南》的相关要求; 3) 灾难恢复预案的教育、培训、演练周期符合要求 |
| 判定原则: 达到以上预期结果, 则通过, 否则不通过 |

5.2 第2级要求

5.2.1 业务安全要求

5.2.1.1 业务认证管理

在按照第1级要求检测基础上，还应检测如下内容：

| |
|---|
| 测试编号：PWLAN-第2级-业务安全要求-业务认证管理-01 |
| 测试项目：《公众无线局域网安全防护要求》5.2.1.1-a，应能防止身份鉴别暴力攻击 |
| <p>测试步骤：</p> <ol style="list-style-type: none"> 1) 检查设计/验收文档，确定系统是否能防止身份鉴别暴力攻击（如，登录模块是否采用随机验证码进行验证，并且保证验证码不易被自动预测、识别等）； 2) 访谈相关技术人员，确定是否有防止身份鉴别暴力攻击的措施； 3) 创建测试账号，并保证账号功能正常； 4) 使用测试账号进行登录测试； 5) 验证模块能防止身份鉴别暴力攻击 |
| <p>预期结果：</p> <ol style="list-style-type: none"> 1) 设计/验收文档中，系统提供了保护措施防止身份鉴别暴力攻击； 2) 相关技术人员确认实际系统提供了保护措施防止身份鉴别暴力攻击； 3) 登录验证模块能防止身份鉴别暴力攻击（如，登录模块采用随机验证码进行验证，并且保证验证码不易被自动预测、识别等） |
| <p>判定原则：</p> <p>达到以上预期结果，则通过，否则不通过</p> |

| |
|--|
| 测试编号：PWLAN-第2级-业务安全要求-业务认证管理-02 |
| 测试项目：《公众无线局域网安全防护要求》5.2.1.1-b，应具有防范利用AP或用户认证报文发起攻击的能力 |
| <p>测试步骤：</p> <ol style="list-style-type: none"> 1) 访问技术人员采用何种措施防范利用AP或用户认证报文发起攻击； 2) 查看监测平台历史记录，是否包括无线泛洪攻击、无线中间人攻击、无线欺骗攻击等监测记录 |
| <p>预期结果：</p> <ol style="list-style-type: none"> 1) PWLAN网络中部署有无线安全设备等措施防范无线攻击； 2) 监测平台历史记录包括对无线攻击事件的检测记录 |
| <p>判定原则：</p> <p>达到以上预期结果，则通过，否则不通过</p> |

5.2.1.2 业务资源控制

在按照第 1 级要求检测基础上，还应检测如下内容：

| |
|--|
| 测试编号：PWLAN-第 2 级-业务安全要求-业务资源控制-01 |
| 测试项目：《公众无线局域网安全防护要求》5.2.1.2 -a，具有防止过度访问、拒绝服务攻击等的保护机制 |
| 测试步骤： 1) 询问技术人员是否具有防止过度访问、拒绝服务攻击等的保护机制； 2) 查看网络设备配置和网络管理平台日志，是否能够识别拒绝服务攻击并有相应的告警机制； 3) 创建测试账号； 4) 使用测试账号过度（超过限制次数）访问无线网络 |
| 预期结果： 1) 过度访问、拒绝服务攻击可以被识别，且具有告警信息上报； 2) 该用户被禁止访问无线网络，且有告警信息上报； 3) 测试账号登录失败，且有告警信息上报 |
| 判定原则： 达到以上预期结果，则通过，否则不通过 |

5.2.1.3 业务安全防范

在按照第 1 级要求检测基础上，还应检测如下内容：

| |
|---|
| 测试编号：PWLAN-第 2 级-业务安全要求-业务安全防范-01 |
| 测试项目：《公众无线局域网安全防护要求》5.2.1.3 -a，应具备防护无线中间人攻击的能力 |
| 测试步骤： 1) 询问技术人员采用何种措施防护无线中间人攻击； 2) 查看监测平台历史记录，是否包含对无线中间人攻击的记录 |
| 预期结果： 1) 部署了无线安全防护设备等措施防护无线中间人攻击； 2) 监测平台历史记录包含对中间人攻击的告警信息 |
| 判定原则： 达到以上预期结果，则通过，否则不通过 |

| |
|--|
| 测试编号: PWLAN-第2级-业务安全要求-业务安全防范-02 |
| 测试项目: 《公众无线局域网安全防护要求》5.2.1.3-b, POATAL 页面应具备防攻击、防篡改的能力 |
| 测试步骤: 1) 访谈技术人员采用了何种措施防止POATAL页面被攻击和篡改; 2) 在URL表单、Cookie等字段进行SQL注入攻击; 3) 判读Portal页面是否能成功抵御SQL注入攻击; 4) 在URL表单、输入框等进行XSS攻击测试尝试; 5) 判读Portal页面是否能成功抵御XSS攻击 |
| 预期结果: 1) Portal 界面不能被 SQL 注入; 2) Portal 界面不能被 XSS 攻击; 3) Portal 页面不能被篡改 |
| 判定原则: 达到以上预期结果, 则通过, 否则不通过 |

5.2.1.4 业务安全审计

在按照第1级要求检测基础上, 还应检测如下内容:

| |
|--|
| 测试编号: PWLAN-第2级-业务安全要求-业务安全审计-01 |
| 测试项目: 《公众无线局域网安全防护要求》5.2.1.4-a, 应具备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: 1) 查看设计文档, 确定PWLAN是否提供对审计记录数据进行统计、查询、分析的功能, 是否提供生成审计报表的功能; 2) 查看实际运行中的审计系统及审计报表; 3) 检查系统是否提供对审计记录数据进行统计、查询、分析的功能; 4) 检查系统是否提供生成审计报表的功能 |
| 预期结果: 1) 在设计中, 系统有对审计记录数据进行统计、查询、分析的功能, 有生成审计报表的功能; 2) 实际系统提供了对审计记录数据进行统计、查询、分析的功能; 3) 实际系统有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 |

5.2.2 设备及软件系统安全要求

5.2.2.1 AC、AP 及热点交换机设备

在按照第1级要求检测基础上，还应检测如下内容：

| |
|---|
| 测试编号：PWLAN-第2级-设备及软件系统安全-AC、AP 及热点交换机设备-01 |
| 测试项目：《公众无线局域网安全防护要求》5.2.2.1-a，使用安全漏洞扫描设备定期对所有 PWLAN 相关设备（AC、Radius、Web Portal 等）进行安全漏洞扫描 |
| 测试步骤： 1) 查看已有漏洞扫描报告； 2) 查看是否使用安全漏洞扫描工具对PWLAN网络设备（AC、Radius、Portal、热点交换机）进行扫描； 3) 查看是否存在高、中风险的安全漏洞； 4) 询问技术人员对相应漏洞的处理办法； 5) 检查是否对漏洞及时修补 |
| 预期结果： 1) 具有漏洞扫描报告，报告显示不存在高危漏洞； 2) 已有的漏洞已经修补 |
| 判定原则： 达到以上预期结果，则通过，否则不通过 |

5.2.2.2 网络设备

同第1级检测要求。

5.2.2.3 数据库

同第1级检测要求。

5.2.2.4 操作系统

同第1级检测要求。

5.2.3 网络安全要求

5.2.3.1 网络拓扑

同第1级检测要求。

5.2.3.2 网络保护与恢复

在按照第1级要求检测基础上,还应检测如下内容:

| |
|---|
| 测试编号: PWLAN-第2级-网络安全-网络保护与恢复-01 |
| 测试项目:《公众无线局域网安全防护要求》5.2.3.2-a, PWLAN 相关关键数据(如,业务数据、配置数据、性能数据、告警数据等)应有本地数据备份 |
| 测试步骤: 1) 访谈网络运维人员和安全管理人員,查看数据备份要求、安全策略、灾难应急预案、数据备份记录等,查看 PWLAN 相关关键数据的备份方式; 2) 检查 PWLAN 相关关键数据(如业务数据、设备配置数据、性能数据、告警数据等)是否有本地数据备份; 3) 通过加载备份数据等方式验证其有效性及恢复能力是否均符合要求 |
| 预期结果: 1) 关键数据(如业务数据、设备配置数据、性能数据、告警数据等)本地备份与设计/验收文档一致; 2) 拥有按介质特性对备份数据定期进行有效性验证的制度; 3) 备份数据能够完成有效性验证并与已经存档的验证记录或报告保持一致 |
| 判定原则: 达到以上预期结果,则通过,否则不通过 |

| |
|---|
| 测试编号: PWLAN-第2级-网络安全-网络保护与恢复-02 |
| 测试项目:《公众无线局域网安全防护要求》5.2.3.2-b, PWLAN 网络灾难备份和恢复时间应满足行业管理、网络和业务运营商应急预案的要求 |
| 测试步骤: 1) 访谈网络运维人员和安全管理人員,检查网络安全策略、灾难应急预案、演练记录等,查看对于不同网络灾难的备份和恢复时间的相关要求; 2) 在业务空闲时段模拟网络故障(链路或设备故障),检查 PWLAN 网络灾难恢复的时间是否能满足行业管理、网络和业务运营商应急预案的要求 |
| 预期结果: 1) PWLAN 在灾难恢复时对应急通信、重要应用和业务网络通信采取了保障措施; 2) 采取的灾难恢复保障措施满足优先保证应急通信、重要应用和业务网络的通信,其次满足恢复一般应用和业务网络通信的要求 |
| 判定原则: 达到以上预期结果,则通过,否则不通过 |

5.2.3.3 网络管理

在按照第1级要求检测基础上，还应检测如下内容：

| |
|--|
| 测试编号：PWLAN-第2级-网络安全-网络管理-01 |
| 测试项目：《公众无线局域网安全防护要求》5.2.3.2-a，PWLAN 网络管理原则上应具有对业务相关数据进行检测、统计、控制、过滤的功能 |
| 测试步骤： 1) 访谈网络运维人员，查看网络管理系统设计文档、设备配置记录等，查看对业务数据的管理情况； 2) 检查网络管理有关设备的管理功能和配置信息，检查其是否启用了安全管理技术手段； 3) 模拟某种业务在 PWLAN 内传送，查看管理系统的反映情况 |
| 预期结果： 1) PWLAN 建有对网络业务数据进行安全管理的技术手段； 2) PWLAN 的网络管理具有对网络业务相关数据进行检测、统计、控制、过滤的功能 |
| 判定原则： 达到以上预期结果，则通过，否则不通过 |

5.2.3.4 网络安全监测

在按照第1级要求检测基础上，还应检测如下内容：

| |
|---|
| 测试编号：PWLAN-第2级-网络安全-网络安全监测-01 |
| 测试项目：《公众无线局域网安全防护要求》5.2.3.4-a，应具备空口无线安全事件监测功能 |
| 测试步骤： 1) 询问技术人员是否具备空口无线安全事件监测功能； 2) 查看监测记录等相关信息，是否包含对空口无线安全事件（如 WLAN DoS 攻击、WLAN HotSpotter 攻击、WLAN 中间人攻击、WLAN 干扰）的监测记录 |
| 预期结果： 1) 支持对上述空口无线安全事件的监测功能； 2) 监测记录包含对安全事件的监测记录 |
| 判定原则： 达到以上预期结果，则通过，否则不通过 |

| |
|--|
| 测试编号: PWLAN-第2级-网络安全-网络安全监测-02 |
| 测试项目: 《公众无线局域网安全防护要求》5.2.3.4-b, 应具备 AP 配置实时监测功能 |
| 测试步骤: 1) 询问技术人员是否具备 AP 配置实时监测功能; 2) 检查 AP 配置实时监测日志 |
| 预期结果: 1) 具有脆弱性风险监测功能; 2) 存有 AP 配置实时监测日志 |
| 判定原则: 达到以上预期结果, 则通过, 否则不通过 |

5.2.3.5 网络安全防范

在按照第1级要求检测基础上, 还应检测如下内容:

| |
|--|
| 测试编号: PWLAN-第2级-网络安全-网络安全防范-01 |
| 测试项目: 《公众无线局域网安全防护要求》5.2.3.5-a, 应防止非授权使用网络 |
| 测试步骤: 1) 访问技术人员采用了何种技术手段防止非授权使用网络; 2) 检查是否设置了防火墙策略, 用于防止 DNS 隧道绕过认证; 3) 模拟 DNS 隧道, 测试是否能够绕过认证机制上网 |
| 预期结果: 1) 设置了防火墙策略; 2) 不存在 DNS 隧道绕过漏洞 |
| 判定原则: 达到以上预期结果, 则通过, 否则不通过 |

| |
|--|
| 测试编号: PWLAN-第2级-网络安全-网络安全防范-02 |
| 测试项目: 《公众无线局域网安全防护要求》5.2.3.5-b, 应防止利用 PWLAN 中网络地址划分安全域隔离缺陷, 导致直接入侵控制 |
| 测试步骤: 1) 访谈 PWLAN 网络管理人员; 2) 查看网络设计文档、安全域隔离配置文档等; 3) 检查安全域隔离划分情况, 验证安全域隔离效果 |
| 预期结果: 1) PWLAN 网络地址划分了安全域隔离; 2) 安全域隔离生效 |
| 判定原则: 达到以上预期结果, 则通过, 否则不通过 |

| |
|--|
| 测试编号: PWLAN-第2级-网络安全-网络安全防范-03 |
| 测试项目: 《公众无线局域网安全防护要求》5.2.3.5-c, 应具有防范通过空口进行的无线拒绝服务攻击的能力 |
| 测试步骤: 1) 询问技术人员采用了何种措施防范通过空口进行的无线拒绝服务攻击; 2) 查看监测记录等相关信息, 是否包含无线拒绝服务攻击记录; 3) 查看安全防护设备能否检测到无线拒绝服务攻击事件 |
| 预期结果: 1) 监测记录包含无线拒绝服务攻击记录; 2) 安全防护设备上报攻击事件, 事件描述包括攻击设备 MAC、时间等信息 |
| 判定原则: 达到以上预期结果, 则通过, 否则不通过 |

| |
|---|
| 测试编号: PWLAN-第2级-网络安全-网络安全防范-04 |
| 测试项目: 《公众无线局域网安全防护要求》5.2.3.5-d, 辅助系统应限制和禁用可能造成漏洞的服务和端口, 在系统边界启用防攻击、防入侵措施, 相关软件应及时安装补丁, 定期检查更新 |
| 测试步骤: 1) 访谈网络运维人员, 检查系统设计/验收文档、系统安全策略、系统管理和配置文档; 2) 检查 PWLAN 系统边界是否安装和使用防火墙和入侵检测等防攻击、防入侵措施; 3) 检查 PWLAN 系统相关软件补丁版本和更新时间; 4) 检查 PWLAN 关联辅助系统的服务和端口设置; 5) 使用端口扫描工具对 PWLAN 关联辅助系统进行端口扫描, 检查是否存在可能造成漏洞的服务和端口 |
| 预期结果: 1) 通用服务器/主机设备的系统软件均限制和禁用可能造成漏洞的服务和端口 (仅开放其提供正常功能所必须的服务端口); 2) 相关的通用主机均安装和使用有效授权的防火墙、入侵检测及病毒查杀工具 (或采取其它防病毒和防攻击措施); 3) 相关联网的通用服务器/主机设备所安装和使用的软件及时安装了补丁、并定期更新; 4) 安全漏洞的检测和修补形成了备查的报告/记录 |
| 判定原则: 达到以上预期结果, 则通过, 否则不通过 |

| |
|---|
| 测试编号: PWLAN-第2级-网络安全-网络安全防范-05 |
| 测试项目: 《公众无线局域网安全防护要求》5.2.3.5-e, PWLAN 和相关系统内部署的安全设备应能及时准确的提供攻击或入侵的报警、监测信息 |
| 测试步骤: 1) 访谈网络运维和安全管理人員, 查看网络安全策略、设备维护记录、故障告警记录、日志文件资料等, 查看 PWLAN 和相关辅助系统应对入侵和攻击的设计; 2) 检查是否部署并启用安全设备; 3) 检查安全设备的日志记录, 查看其是否记录有对攻击或入侵的报警和监测信息 |
| 预期结果: 1) PWLAN 和相关辅助系统内部署并启用安全设备; 2) 发生攻击或入侵时, 安全设备能及时、准确的提供相关类型攻击、入侵的报警和监测信息 |
| 判定原则: 达到以上预期结果, 则通过, 否则不通过 |

| |
|---|
| 测试编号: PWLAN-第2级-网络安全-网络安全防范-06 |
| 测试项目: 《公众无线局域网安全防护要求》5.2.3.5-f, PWLAN 各类设备及系统应启用完整的安全日志功能, 并实现日志的管理和安全审计 |
| 测试步骤: 1) 访谈网络安全管理人员, 查看网络安全策略、设备维护记录、日志记录、审计文件资料等, 查看各类设备及系统安全日志和审计相关功能; 2) 检查 PWLAN 各类设备及系统是否均启用安全日志的功能; 3) 检查 PWLAN 各类设备及系统是否定期对各类日志信息进行审计 |
| 预期结果: 1) PWLAN 各类设备及系统具有并启用了安全日志功能; 2) 安全日志能完整记录安全相关事件的来源、时间、事件描述等要素信息和内容; 3) 日志记录覆盖了维护、管理用户相关登录访问类事件、操作维护类事件, 覆盖了设备相关状态监测、统计类事件、故障告警类事件; 4) 日志记录保存时间不少于 90 天; 5) 日志按照管控策略要求进行安全管理, 并定期审计, 审计记录保存时间是否不少于 180 天 |
| 判定原则: 达到以上预期结果, 则通过, 否则不通过 |

| |
|--|
| 测试编号: PWLAN-第2级-网络安全-网络安全防范-07 |
| 测试项目: 《公众无线局域网安全防护要求》5.2.3.5-g, 不应出现 Owasp Top10 所列的高危 Web 安全漏洞 |
| 测试步骤: 1) 询问技术人员是否存在 Owasp Top10 所列的高危 Web 安全漏洞; 2) 通过漏洞扫描等手段检查是否存在 Owasp Top10 高危漏洞; 3) 通过渗透技术检测是否存在 Owasp Top10 高危漏洞; 4) 通过检测 PWLAN 登录网站的配置和软件版本检测是否存在 Owasp Top10 漏洞 |
| 预期结果: 1) 渗透、扫描检查无 Owasp Top10 高危漏洞; 2) 配置和软件比对无 Owasp Top10 高危漏洞风险 |
| 判定原则: 达到以上预期结果, 则通过, 否则不通过 |

5.2.4 物理环境安全要求

在按照第1级要求检测基础上，还应检测如下内容：

| |
|--|
| 测试编号：PWLAN-第2级-物理环境安全要求-01 |
| 测试项目：《公众无线局域网安全防护要求》5.2.4-a，应满足 YD/T 1754-2008《电信网和互联网物理环境安全等级保护要求》中第2级的相关要求 |
| 测试步骤： 按照 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》中第2级的相关要求进行检测 |
| 预期结果： 符合 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》中第2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 |

5.2.5 管理安全要求

在按照第1级要求检测基础上，还应检测如下内容：

| |
|--|
| 测试编号：PWLAN-第2级-管理安全要求-01 |
| 测试项目：《公众无线局域网安全防护要求》5.2.5-a，应满足 YD/T 1756-2008《电信网和互联网管理安全等级保护要求》中第2级的相关要求 |
| 测试步骤： 按照 YD/T 1757-2008《电信网和互联网管理安全等级保护检测要求》中第2级的相关要求进行检测 |
| 预期结果： 符合 YD/T 1757-2008《电信网和互联网管理安全等级保护检测要求》中第2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 |

| |
|---|
| 测试编号: PWLAN-第2级-管理安全要求-02 |
| 测试项目:《公众无线局域网安全防护要求》5.2.5-b, 应定期对PWLAN各类设备、系统进行安全风险评估 |
| 测试步骤: 1) 访谈网络安全管理人员, 查看风险评估报告, 查看PWLAN及其所属各类设备、系统的风险评估情况; 2) 检查是否针对PWLAN网络设备、系统进行定期安全风险评估; 3) 检查风险评估周期是否符合要求 |
| 预期结果: 1) 风险评估报告、风险处理计划和报告、安全加固和升级记录完好; 2) PWLAN网络设备、系统定期进行安全风险评估; 3) 安全风险评估的周期满足至少每两年一次, 重大活动节日前应进行评估 |
| 判定原则: 达到以上预期结果, 则通过, 否则不通过 |

| |
|--|
| 测试编号: PWLAN-第2级-管理安全要求-03 |
| 测试项目:《公众无线局域网安全防护要求》5.2.5-c, PWLAN 应设有专职的操作、维护技术人员和安全管理人員, 应定期组织对相关人员进行技术培训和考核 |
| 测试步骤: 1) 访谈网络运维技术人员和安全管理人員, 查看人員岗位要求、培训教育和考核要求、教育和考核记录等, 查看相关人員岗位管理情况; 2) 检查PWLAN是否设有专职的操作、维护技术人员和安全管理人員岗位; 3) 检查是否定期组织对有关人員进行技术培训和考核 |
| 预期结果: 1) PWLAN 设有专职的设备和网络操作、维护的技术人員和安全管理相关人員; 2) 对相关管理、技术人員进行定期的培训和考核并有记录可查; 3) 对相关管理和技术人員的定期技术培训和考核结果符合岗位要求 |
| 判定原则: 达到以上预期结果, 则通过, 否则不通过 |

| |
|---|
| 测试编号: PWLAN-第 2 级-管理安全要求-04 |
| 测试项目:《公众无线局域网安全防护要求》5.2.5-d, 应定期组织 PWLAN 各类设备、系统灾难恢复预案的教育培训和演练。 |
| 测试步骤: 1) 访谈网络安全管理人员, 查看网络灾难恢复预案、预案教育培训和演练记录等; 2) 检查和验证灾难恢复预案的教育、培训、演练周期是否符合要求 |
| 预期结果: 1) 灾难恢复预案与设计/验收文档一致, 有明确的作用范围, 指定了灾难恢复的目标, 包含灾难恢复的整个过程; 2) 灾难恢复预案有评审报告, 通过决策层的审核和批准, 确定为正式执行文件; 3) 定期进行灾难恢复预案的教育培训; 4) 定期进行灾难恢复预案的演练; 5) 灾难恢复预案的教育培训、演练均留有记录 |
| 判定原则: 达到以上预期结果, 则通过, 否则不通过 |

| |
|---|
| 测试编号: PWLAN-第 2 级-管理安全要求-05 |
| 测试项目:《公众无线局域网安全防护要求》5.2.5-e, 应定期对 PWLAN 空口信号进行安全风险评估 |
| 测试步骤: 1) 询问技术人员对PWLAN空口信号进行安全风险评估的情况; 2) 查看风险评估报告, 检查是否定期对PWLAN空口信号进行无线安全风险评估 |
| 预期结果: 具有风险评估报告, 无线安全风险评估符合要求 |
| 判定原则: 达到以上预期结果, 则通过, 否则不通过 |

5.3 第3级要求

5.3.1 业务安全要求

同第2级检测要求。

5.3.2 设备及软件系统安全要求

同第2级检测要求。

5.3.3 网络安全要求

同第2级检测要求。

5.3.4 物理环境安全要求

同第2级检测要求。

5.3.5 管理安全要求

在按照第2级要求检测基础上，还应检测如下内容：

| |
|---|
| 测试编号：PWLAN-第3级-管理安全要求-01 |
| 测试项目：《公众无线局域网安全防护要求》5.3.5-a，应定期对PWLAN各类设备、系统进行安全风险 评估 |
| 测试步骤： 1) 访谈网络安全管理人员，查看风险评估报告，查看PWLAN及其所属各类设备、系统的风险评估情况； 2) 检查是否针对PWLAN网络设备、系统进行定期安全风险评估； 3) 检查风险评估周期是否符合要求 |
| 预期结果： 1) 风险评估报告、风险处理计划和报告、安全加固和升级记录完好； 2) PWLAN网络设备、系统定期进行安全风险评估； 3) 安全风险评估的周期满足至少每年一次，重大活动节日前应进行评估 |
| 判定原则： 达到以上预期结果，则通过，否则不通过 |

5.4 第4级要求

待补充。

5.5 第5级要求

待补充。

中华人民共和国
通信行业标准
公众无线局域网安全防护检测要求
YD/T 2697-2014

*

人民邮电出版社出版发行
北京市丰台区成寿寺路11号邮电出版大厦
邮政编码：100164
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 2014年11月第1版
印张：3.25 2014年11月北京第1次印刷
字数：84千字

15115·483

定价：35元

本书如有印装质量问题，请与本社联系 电话：(010)81055492