ICS 35.040
L 80

中华人民共和国国家标准

GB/T 30282—2013

信息安全技术
反垃圾邮件产品技术要求和测试评价方法

Information security technology—Techniques requirements and testing and evaluation approaches for Anti-Spam product

2013-12-31 发布　　2014-07-15 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由全国信息安全标准化技术委员会(SAC/ TC 260)提出并归口。

本标准起草单位:中国信息安全认证中心、上海市信息安全测评认证中心。

本标准主要起草人:布宁、陈清明、甘杰夫、张俊彦、贾雪飞、李菁。

引　言

为指导反垃圾邮件产品的研制、生产、测试和评价工作的开展，本标准依据 GB/T 18336—2008《信息技术　安全技术　信息技术安全性评估准则》，从反垃圾邮件产品的功能、自身安全和安全保证等几个方面提出了相关技术要求，并提出了测试评价方法。

信息安全技术
反垃圾邮件产品技术要求和测试评价方法

1 范围

本标准规定了反垃圾邮件产品的技术要求和测试评价方法。

本标准适用于反垃圾邮件产品的设计、开发、测试和评价。

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(idt ISO/IEC 2382-8：1998)

GB/T 18336.1—2008 信息技术 安全技术 信息技术安全性评估准则 第1部分：简介和一般模型(ISO/IEC 15408-1：2005，IDT)

GB/T 18336.2—2008 信息技术 安全技术 信息技术安全性评估准则 第2部分：安全功能要求(ISO/IEC 15408-2：2005，IDT)

GB/T 18336.3—2008 信息技术 安全技术 信息技术安全性评估准则 第3部分：安全保证要求(ISO/IEC 15408-3：2005，IDT)

3 术语和定义

GB/T 5271.8—2001 和 GB/T 18336.1—2008 界定的以及下列术语和定义适用于本文件。

3.1

垃圾邮件 spam

电子邮件使用者事先未提出要求或同意接收的电子邮件，一般具有如下特征：

——未经电子邮件使用者请求而发送；

——同时发送给大量用户；

——伪造的发件人信息。

3.2

反垃圾邮件产品 anti-spam product

能够对垃圾邮件进行识别和处理的软件或软硬件组合，包括透明的反垃圾邮件网关、基于转发的反垃圾邮件系统、安装于邮件服务器的反垃圾邮件软件，以及与邮件服务器一体的反垃圾邮件的邮件服务器等。

3.3

黑名单 blacklist

电子邮件使用者不想接收到的发件人的邮件地址列表。

3.4

实时黑名单 realtime blacklist

由第三方机构和组织收集并维护的经常发送垃圾电子邮件的邮件地址列表。

3.5

虚假路由　false routing

邮件中声明的域名所对应的网络地址与该邮件实际来源网络地址不符。

3.6

投递　send

反垃圾邮件产品不对邮件进行过滤等处理，直接发送给收件人。

3.7

标记投递　label and send

反垃圾邮件产品将邮件标记为垃圾邮件后发送给收件人。

3.8

隔离　isolate

反垃圾邮件产品将识别为垃圾邮件或不应专递至使用者的邮件放置到专用的存储区域。

3.9

拒绝　reject

反垃圾邮件产品不接收邮件，并通知发件人该邮件被拒收。

3.10

丢弃　discard

反垃圾邮件产品将邮件直接拦截而不通知发件人。

4　反垃圾邮件产品等级划分

根据产品功能要求和安全保证要求的不同，以及反垃圾邮件产品适用应用环境的不同，将反垃圾邮件产品分为基本级和增强级两个等级。基本级评估保障要求达到 EAL2 级（见 GB/T 18336.3—2008），可适用家庭、小型企业或机构等反垃圾邮件需求比较简单的环境。增强级评估保障要求达到 EAL3 级（见 GB/T 18336.3—2008），可适用中、大型企业或机构等反垃圾邮件需求比较综合的环境。产品等级划分如表 1 所示。

表 1　反垃圾邮件产品等级划分表

技术要求			基本级	增强级
功能要求	垃圾邮件识别	基于邮件网络地址的垃圾邮件识别	*	**
		基于邮件内容特征的垃圾邮件识别	*	**
		基于邮件连接特征的垃圾邮件识别	*	**
	垃圾邮件处理		*	**
	管理控制功能	策略配置	*	*
		网络部署	*	*
		产品升级	*	**
	报表统计		*	*
安全要求	安全审计	审计数据生成	*	*
		审计数据查阅	*	*
		审计数据存储	*	*

表 1（续）

技 术 要 求		基本级	增强级
安全要求	身份鉴别	*	*
	用户角色	*	*
	远程会话保护	*	*
保证要求	配置管理	*	**
	交付与运行	*	*
	开发	*	**
	指导性文档	*	*
	测试	*	**
	脆弱性评定	*	*
注：“*”和“**”表示产品应具备该项技术要求。“*”表示两个级别产品对于该项技术要求相同；“**”表示增强级产品相对于基本级产品在这项技术要求上进行了增强。标准正文中，若某些内容采用**加粗**字体，则表示该部分内容只对增强级产品提出要求或该部分内容中增强级产品相对于基本级产品进行了增强。			

5 技术要求

5.1 功能要求

5.1.1 垃圾邮件识别

反垃圾邮件产品应至少采用以下一种技术手段来识别垃圾邮件。

5.1.1.1 基于邮件发送地址的垃圾邮件识别

反垃圾邮件产品应能依据邮件发送方邮件地址来判断邮件是否为垃圾邮件，可采用黑名单、实时黑名单、虚假路由识别等技术方式实现。

a) 应提供黑名单的编辑（添加、删除等）功能，也可导入导出黑名单；

b) **支持和邮件客户端、邮件服务器之间的联动，邮件客户端的用户在手动阻止发件人之后能够将被阻止的发件人邮件地址同步至反垃圾邮件产品的黑名单中；**

c) 支持实时黑名单功能，可通过 DNS（Domain Name Server，域名服务器）查询方式来查询黑名单列表。

5.1.1.2 基于邮件内容特征的垃圾邮件识别

反垃圾邮件产品应能依据以下邮件内容特征来识别邮件是否为垃圾邮件：

a) 关键字过滤识别：可针对邮件的信头、信体、附件、主题、发件人、收件人、抄送人、正文中包含的文字而设定关键字，从而匹配识别垃圾邮件；

b) 数值特征匹配识别：可设定邮件或附件的大小、附件的数量、收件人总数等数量值，进行匹配识别垃圾邮件；

c) 附件特征匹配识别：根据附件文件名和附件文件类型等特征进行垃圾邮件识别；

d) **应能识别出带病毒特征的邮件附件；**

e) 其他特征识别。

5.1.1.3 基于邮件连接特征的垃圾邮件识别

反垃圾邮件产品应能依据以下邮件连接特征判断是否有发送垃圾邮件的行为：

a) 一段时间内同一主题的邮件接收次数；

b) **同一邮件来源 IP 地址对邮件服务端口的最大并发连接数量；**

c) **一段时间内同一邮件来源 IP 地址对邮件服务端口的最大连接数；**

d) 其他连接特征。

5.1.2 垃圾邮件处理

反垃圾邮件产品应提供以下可供选择的垃圾邮件处理方式：

a) 投递；

b) 标记投递；

c) 隔离，**并允许邮件用户登录到隔离区，恢复自己的邮件；**

d) 拒绝；

e) 丢弃。

5.1.3 管理控制功能

5.1.3.1 策略配置

应提供方便、快捷的垃圾邮件识别的配置方法和手段。

5.1.3.2 网络部署方式

网关类反垃圾邮件产品应支持透明方式和路由方式的接入。

5.1.3.3 产品升级

a) 反垃圾邮件产品应可通过手动或 Internet 自动的方式及时更新垃圾邮件规则库**和新病毒特征码；**

b) **自动升级时，产品应能对升级包进行校验，防止升级包被篡改或替换。**

5.1.4 报表统计

反垃圾邮件产品应能将邮件处理结果生成报表，提供灵活多样的统计查询结果，便于对垃圾邮件传递情况进行分析管理。

5.2 自身安全要求

5.2.1 安全审计

5.2.1.1 审计数据生成

反垃圾邮件产品应对以下安全事件生成审计记录：

a) 对安全策略(如邮件过滤策略等)进行更改的操作；

b) 授权管理员的登录和退出；

c) 因鉴别尝试不成功的次数超出了设定的限值，导致会话连接终止；

d) 对用户角色进行增加、删除和属性修改的操作；

e) 读取、修改、破坏审计数据的尝试；
f) 对其他安全功能配置参数的修改(设置和更新)，无论成功与否；
g) 能对垃圾电子邮件过滤和阻断行为进行记录，记录内容至少包括发件人网络地址和邮件地址、收件人地址、邮件主题、发信时间、阻断原因等信息。

5.2.1.2 审计数据查阅

反垃圾邮件产品应：

a) 只允许授权用户访问审计数据；
b) 提供对审计数据的查询功能，能按照条件或条件组合进行查询；
c) 提供相应的统计分析功能，方便用户掌握垃圾邮件状况，以便及时采取防护措施。

5.2.1.3 审计数据存储

a) 产品应提供审计数据的导出和转存功能，以保证产品有足够的审计数据存储空间；
b) **反垃圾邮件产品应能设置存储空间的阈值，**当达到存储空间阈值时，向管理员进行报警；在审计存储空间耗尽等异常情况下，应能采取相应措施保证(如覆盖以前数据、忽略新产生数据等)已存储审计数据的可用性。

5.2.2 身份鉴别

反垃圾邮件产品应：

a) 对授权管理员至少采用一种身份鉴别方式(如用户名＋口令)进行身份鉴别，**且身份鉴别方式应至少采取“字母和数字”组合的方式；**
b) 为授权管理员和用户登录设定一个可修改的鉴别尝试阈值，当不成功登录尝试超过阈值，反垃圾邮件产品应通过技术手段终止其与产品之间的会话过程。

5.2.3 用户角色

反垃圾邮件产品应定义不同的角色，每个角色可以具有多个用户，但每个用户只能属于一个角色。

5.2.4 安全功能数据传输保护

如果反垃圾邮件产品支持远程管理，应采取安全措施来保护安全功能数据传输。

5.3 安全保证要求

5.3.1 配置管理

5.3.1.1 配置管理能力

a) 开发者应为产品提供一个参照号，并在产品上进行标记，该参照号对产品的每一个版本应是唯一的；
b) 开发者应使用一个配置管理系统。配置管理系统应唯一标识产品所包含的所有配置项，**且应提供措施使得只能对配置项进行授权改变；**
c) **开发者应提供配置管理文档。配置管理文档应描述用于唯一标识产品所包含配置项的方法，并应提供所有配置项都已经或正在配置管理系统下进行有效维护的证据。配置管理文档应包括一个配置清单和一个配置管理计划。配置清单应唯一标识组成产品的所有配置项，并应描述组成产品的配置项。配置管理计划应描述配置管理系统是如何使用的，且应提供证实配置管理系统的运行与配置管理计划是一致的证据。**

5.3.1.2 配置管理范围

开发者应提供一个产品配置项列表。配置项列表应包括:实现表示和安全目标中其他保证组件所要求的评估证据。

5.3.2 交付与运行

5.3.2.1 交付

a) 开发者应使用交付程序给用户交付产品或其部分;
b) 开发者应采用文档的形式描述交付程序,该文档应描述在向用户方分发产品的各个版本时,用以维护其安全性所必需的所有程序。

5.3.2.2 安装、生成和启动

开发者应提供文档描述产品安全地安装、生成和启动必需的所有步骤。

5.3.3 开发

5.3.3.1 功能规范

开发者应提供功能规范的设计文档,该文档应满足如下要求:
a) 对产品功能、安全功能及其外部接口进行非形式化描述;
b) 保证其内在一致性;
c) 描述所有外部安全功能接口的用途与使用方法,适当时提供效果、例外情况和出错消息的细节;
d) 完备地表示产品功能和安全功能。

5.3.3.2 高层设计

开发者应提供产品安全功能的高层设计文档,该文档应满足如下要求:
a) 以非形式化方式表述,并且是内在一致的;
b) 按照子系统来描述产品安全功能的结构;
c) 描述每个产品安全功能子系统所提供的安全功能性;
d) 标识产品安全功能所要求的任何基础性的硬件、固件或软件,以及在这些硬件、固件或软件中实现的支持性保护机制提供功能的一个表示;
e) 标识产品安全功能子系统的所有接口;
f) 标识产品安全功能子系统的哪些接口是外部可见的;
g) 描述产品安全功能子系统所有接口的用途与使用方法,适当时提供效果、例外情况和出错消息的细节;
h) 把产品分成安全策略实施和其他子系统来描述。

5.3.4 指导性文档

5.3.4.1 管理员指南

a) 开发者应提供针对系统管理员的管理员指南。该指南应说明以下内容:
1) 管理员可使用的管理功能和接口;
2) 如何以安全的方式管理产品;

3） 一些关于安全处理环境中应被控制的功能和特权的警示信息；
4） 所有关于与产品安全运行有关用户行为的假设；
5） 所有受管理员控制的安全参数，适当时应指明安全值；
6） 每一种与需要执行的管理功能有关的安全相关事件，包括改变安全功能所控制实体的安全特性；
7） 所有与管理员有关的 IT 环境安全要求。

b） 管理员指南应与供评估的所有其他文档保持一致。

5.3.4.2 用户指南

a） 开发者应提供用户指南。该指南应说明以下内容：
1） 产品的非管理员用户可使用的功能和接口；
2） 产品所提供的用户可访问安全功能的使用；
3） 一些关于安全处理环境中应被控制的用户可访问功能和特权的警示信息；
4） 产品安全运行所必需的所有用户职责，包括与产品安全环境陈述中可找到的与关于用户行为的假设有关的那些职责；
5） 所有与用户有关的 IT 环境安全要求。

b） 用户指南应与供评估的所有其他文档保持一致。

5.3.5 测试

5.3.5.1 测试覆盖

a） 开发者应提供测试覆盖的证据，该证据应说明测试文档中所标识的测试与功能规范中所描述的安全功能之间的对应性；

b） 开发者应提供测试覆盖的一个分析，该分析应证实功能规范中所描述安全功能和测试文档所标识的测试之间的对应性是完备的。

5.3.5.2 功能测试

a） 开发者应测试安全功能，并文档化测试结果；
b） 开发者应提供测试文档，测试文档应包括测试计划、测试程序描述、预期测试结果和实际测试结果；
c） 测试计划应标识要测试的安全功能和描述要执行的测试目标；
d） 测试程序描述应标识要执行的测试，并描述每个安全功能的测试脚本。这些脚本应包括对于其他测试结果的任何顺序依赖性；
e） 预期的测试结果应指出测试成功执行后的预期输出；
f） 开发者执行测试所得到的测试结果应证实每个被测试的安全性功能都按照规定运转。

5.3.5.3 独立性测试

a） 开发者应提供用于测试的产品，该产品应适合测试；
b） 开发者应提供一组相当的资源，用于开发者的产品安全功能测试。

5.3.6 脆弱性评定

5.3.6.1 脆弱性分析

开发者和评估者应执行脆弱性分析，并提供脆弱性分析文档。该文档满足如下要求：

a) 描述为搜索用户能违反产品安全策略的明显方法而执行的产品可交付材料分析；
b) 描述对明显的脆弱性的处置；
c) 针对所有已标识的脆弱性，说明脆弱性不能在产品的预期使用环境中被利用。

6 测试评价方法

6.1 测试环境

反垃圾邮件产品的典型测试环境如图 1 所示。

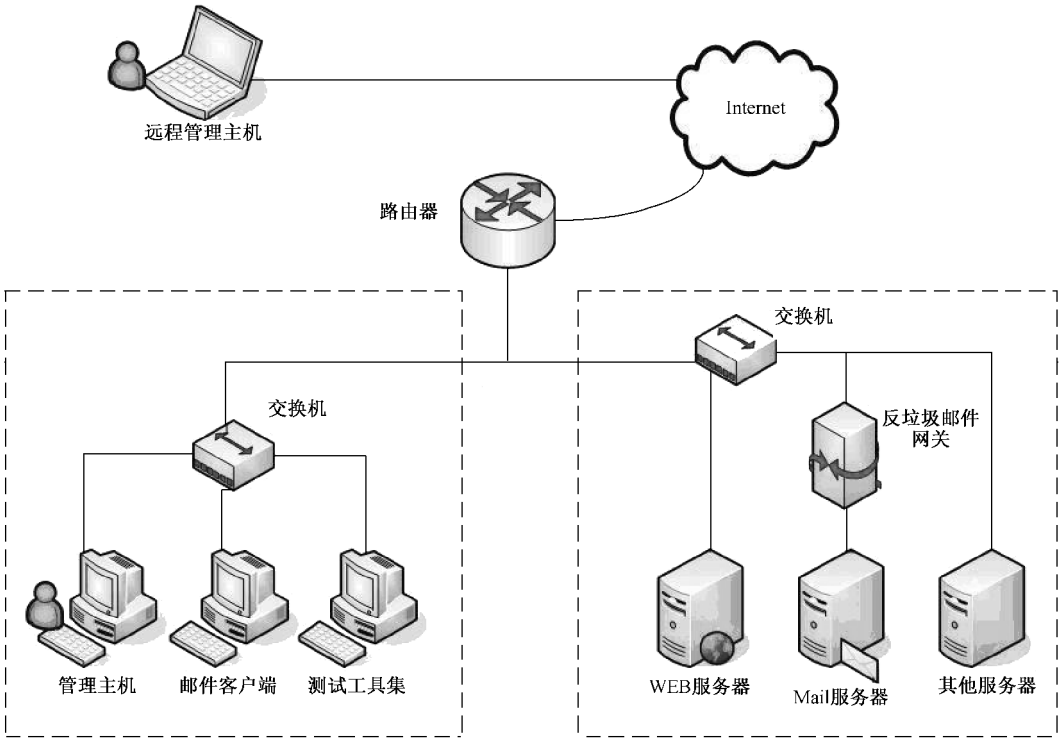

图 1 反垃圾邮件产品典型测试环境示意图

测试设备包括测试所需的交换机、路由器、WEB 服务器、Mail 服务器、反垃圾邮件产品管理主机等。

可用的测试工具包括但不限于：能够制作和发送垃圾邮件的测试工具集等。

6.2 功能测试

6.2.1 垃圾邮件识别

6.2.1.1 基于邮件发送地址的垃圾邮件识别

根据产品采取的垃圾邮件识别机制，可分别或综合采取以下测试方法。

6.2.1.1.1 黑名单

a) 测试方法
1) 配置反垃圾邮件产品的黑名单列表，并验证黑名单设置的有效性。
2) 手工添加、删除黑名单，导入/导出黑名单，检查产品是否具有黑名单编辑功能。

3） **邮件客户端手工阻断正在接收的邮件，并尝试将该发件人邮件地址同步到反垃圾邮件产品黑名单中，验证产品和邮件客户端以及邮件服务器之间的联动。**

4） 查看黑名单内容。

b） 预期结果

1） 产品根据设定的邮件处理方式对黑名单用户发送的邮件进行处理，邮件接收客户端无法接收到其发送过来的邮件。

2） 可以手工编辑黑名单，并可将文件导入/导出黑名单。

3） **被阻止的发件人邮件地址同步至反垃圾邮件产品的黑名单中。**

4） 黑名单采取 IP 地址或邮件地址的形式。

6.2.1.1.2 实时黑名单

a） 测试方法

1） 检查产品是否能够进行提供实时黑名单服务域名的添加、修改等操作。

2） 验证产品所启用的实时黑名单功能的有效性。

b） 预期结果

1） 产品支持主要实时黑名单服务第三方提供的实时黑名单列表。

2） 可以对实时黑名单列表中用户发送的邮件进行阻断。

6.2.1.1.3 虚假路由邮件识别

a） 测试方法

1） 在测试环境中 Intranet 区域设置一台与模拟客户端不在同一网段的客户端主机，设定其邮件域名地址与模拟客户端一致，并向域内其他用户发送邮件。

2） 观察反垃圾邮件产品是否能识别并限制该邮件的发送。

b） 预期结果

反垃圾邮件产品应能识别并阻断虚假路由邮件的发送。

6.2.1.2 基于邮件内容特征的垃圾邮件识别

a） 测试方法

1） 分别针对邮件信头、信体、附件、主题、发件人、收件人、抄送人、暗送人（只针对外发邮件）、邮件正文设定不同的关键字，自邮件客户端向邮件服务器发送含有设定关键字的邮件。

2） 分别设置限制邮件大小、附件的尺寸、附件的数量、收件人总数等特征阀值，自邮件客户端向邮件服务器发送超过设定阀值的邮件。

3） 设定可限制的附件文件名和附件类型（如.doc），自邮件客户端向邮件服务器发送带有所限制附件文件名或附件类型的邮件。

4） **自邮件客户端向邮件服务器发送带有病毒特征附件的邮件。**

5） 按“与”“或”“非”的逻辑关系组合上述设定限制条件，自邮件客户端向邮件服务器发送具有所设定组合条件的邮件。

6） 分别判断产品是否能对上述邮件进行过滤。

7） 审查产品说明书分析产品是否采用以上特征以外的静态特征过滤机制，并采取相应的验证措施，证明产品对垃圾邮件的识别和过滤。

b） 预期结果

反垃圾邮件产品能根据所设定的邮件关键字、邮件数值特征和附件特征及其组合条件分别对邮件进行扫描过滤。

6.2.1.3 基于邮件连接特征的垃圾邮件识别

a) 测试方法

1) **设定反垃圾邮件产品允许同一邮件来源 IP 地址的最大并发连接数，使用测试工具集向邮件服务器并发超过设定连接数的邮件。**

2) **设定反垃圾邮件产品可允许的一段时间内同一邮件来源 IP 地址的最大连接数，使用测试工具集不断向邮件服务器发送超过设定次数的邮件，直至达到设定时间。**

3) 设定一段时间内某一主题邮件的接受次数，自邮件客户端在限定时间段内向邮件服务器发送带有限定主题的邮件，直至达到限定次数。

4) 观察以上过程中产品是否能自动阻断新的连接。

5) 审查产品说明书，分析产品是否具有以上限制功能以外的邮件过滤机制，并采取相应的验证措施，证明产品对垃圾邮件的识别和过滤。

b) 预期结果

反垃圾邮件产品在达到设定的限定条件时能够自动进行阻断邮件客户端所发送的邮件。

6.2.2 垃圾邮件处理

a) 测试方法

1) 审查产品说明书是否具有对垃圾邮件处理方式的描述，并在产品中选取不同的处理方式；

2) 由邮件客户端向邮件服务器发送一定数量垃圾邮件，分别验证产品对垃圾邮件的不同处理方式和处理结果；

3) **邮件客户端收件人尝试登录邮件服务器隔离区恢复被隔离的邮件。**

b) 预期结果

1) 产品对垃圾邮件的处理应至少包括：投递、标记投递、隔离、拒绝、丢弃等方式；

2) **邮件客户端收件人可以登录隔离区恢复被隔离的邮件。**

6.2.3 管理控制功能

6.2.3.1 策略配置

a) 测试方法

1) 按照产品说明书，查看产品使用的默认策略。

2) 验证是否可以编辑或修改生成新的策略。

b) 预期结果

1) 产品应提供默认的垃圾邮件识别策略。

2) 应允许授权用户编辑策略。

3) 具有供用户编辑策略的向导功能。

4) 支持策略的导入和导出。

6.2.3.2 网络部署方式

a) 测试方法

检查产品说明书和测试配置环境，判断产品所支持的网络接入方式，并在测试环境中调试其网络接入的有效性。

b) 预期结果

网关类产品应提供透明接入方式和路由接入方式。

6.2.3.3 产品升级

a) 测试方法

1) 检查垃圾邮件规则库的升级方式。

2) **检查病毒特征库的升级方式。**

b) 预期结果

垃圾邮件规则库**和病毒特征库**可以通过手动升级或者自动的在线升级；**自动升级时应能采取签名等校验机制，避免得到错误或伪造的升级包。**

6.2.4 报表统计

a) 测试方法

1) 查验产品对垃圾邮件处理结果的报告生成功能，并查看所生成报告的内容。

2) 查验报告结果的查询统计功能。

b) 预期结果

1) 反垃圾邮件产品具有垃圾邮件处理结果报告生成功能。

2) 可以对生成的报告结果按照表格、柱状图、饼图等形式进行表现。

3) 可以邮件发送时间、发件人地址、收件人地址等进行查询统计。

6.3 自身安全测试

6.3.1 安全审计

6.3.1.1 审计数据生成

a) 测试方法

1) 更改内容过滤等过滤策略，审查审计记录。

2) 授权管理员登录并退出，审查审计记录。

3) 多次尝试不成功的登录操作，审查审计记录。

4) 进行用户管理操作，添加、删除用户，修改用户口令等，审查审计记录。

5) 读取并尝试修改审计记录，审查审计记录。

6) 自邮件客户端向邮件服务器分别发送一定数量的基于内容过滤和地址过滤的垃圾邮件，审查产品是否记录相应拦截和阻断结果。并查阅记录内容是否包括网络地址和邮件地址、收件人地址、邮件主题、发信时间、阻断原因等信息。

b) 预期结果

1) 对每一个测试都产生正确的审计记录。

2) 产生的审计记录与其发生的事件相对应。

6.3.1.2 审计数据查阅

a) 测试方法

1) 查验审计数据是否只允许授权用户进行访问。

2) 审查产品是否能对审计记录内容进行分类查询和分类统计。

b) 预期结果

1) 只有授权用户才能访问审计记录。

2) 可以按照不同字段进行分类查询。

3) 可以对审计记录内容根据不同字段进行分类统计。

6.3.1.3 审计数据存储

a) 测试方法

1) 查验产品对审计数据可用性的保护机制，并验证保护机制的有效性；
2) 查验产品对存储空间阈值设置功能和超出阈值后的报警方式；
3) 验证产品是否提供将审计数据导出和转存的功能。

b) 预期结果

1) 产品提供授权用户将审计数据以文件方式导出。
2) 产品能设置存储空间的阈值，当达到阈值时，向管理员进行报警。
3) 产品提供可选择的操作以处理审计数据存储空间满的问题，如覆盖以前记录等。

6.3.2 身份鉴别

a) 测试方法

1) 登录产品，检查是否在执行所有功能之前要求首先进行身份认证。
2) **检查产品采取的用户登录鉴别方式，检查其用户名和口令的复杂要求程度。**
3) 检查产品是否定义用户鉴别尝试的最大允许失败次数以及相应的措施（如锁定该帐号、限定登录 IP 地址等）。
4) 尝试多次失败的用户鉴别行为，检查产品是否采取了相应措施，并生成了审计记录。

b) 预期结果

1) 在用户执行任何与安全功能相关的操作之前都应对用户进行鉴别。
2) **用户名和口令应在长度、字母组合等方面有所要求。**
3) 产品应能定义用户鉴别尝试的最大允许失败次数，以及达到失败次数时采取的相应措施，锁定帐号、限定登录 IP 等。
4) 当用户鉴别尝试失败连续达到指定次数后，应采取相应当措施，并生成审计记录。
5) 最大失败次数应仅由授权管理员设定。

6.3.3 用户角色

a) 测试方法

1) 检查产品是否允许定义多个角色。
2) 检查各角色是否可以进行权限划分，内容过滤策略和黑名单更新等操作权限与日志查阅管理等权限是否明确划分。

b) 预期结果

1) 产品允许定义多个角色。
2) 每个角色可以具有多个用户，每个用户只属于一个角色。
3) 反垃圾邮件产品能够保证任何用户标识全局唯一。

6.3.4 安全功能数据传输保护

a) 测试方法

审查产品说明手册并测试，当产品需要通过网络进行远程管理时，是否能提供对安全功能数据进行安全传输的功能。

b) 预期结果

当反垃圾邮件产品需要通过网络进行远程管理时，产品应能对安全功能数据进行保密传输。

6.4 安全保证要求评估

6.4.1 配置管理

6.4.1.1 配置管理能力

a) 评估方法

1) **检查每个版本的产品是否具有唯一的参照号。**

2) **检测产品提供的配置管理系统，验证其是否能唯一标识产品所包含的所有配置项，是否提供措施使得对配置项只能进行授权修改。**

3) **审查产品的配置管理文档中是否包括了配置清单和配置计划，审查配置清单是否描述并唯一标识了组成产品的所有配置项，审查配置计划是否描述了配置管理系统使用方法以及配置管理系统的运作和配置管理计划是否相一致，审查配置管理文档是否描述用于唯一标识产品所包含配置项的方法，是否提供所有配置项都已经和正在配置管理系统下有效地进行维护的证据。**

b) 预期结果

审查记录以及最后结果应(符合/不符合)符合评估方法要求，开发者应提供唯一版本号，开发者提供的配置管理内容应完整。

6.4.1.2 配置管理范围

a) 评估方法

审查开发者是否提供了产品配置项列表，且配置项列表包括：实现表示和安全目标中其他保证组件所要求的评估证据。

b) 预期结果

审查记录以及最后结果(符合/不符合)符合评估方法要求。

6.4.2 交付与运行

6.4.2.1 交付

a) 评估方法

1) 审查产品的交付文档，查看其是否具有安装文档、产品生成文档、指导用户进行产品运维的文档以及产品培训手册等文档；

2) 审查开发者是否提供了交付程序，该程序是否在文档中得到描述。

b) 预期结果

审查记录以及最后结果(符合/不符合)符合评估方法要求，开发者应提供完整的文档描述所有交付的过程(文档和程序交付)。

6.4.2.2 安装、生成和启动

a) 评估方法

审查开发者是否提供了文档描述了产品安全的安装、生成和启动所必要的步骤。

b) 预期结果

审查记录以及最后结果(符合/不符合)符合评估方法要求，安装、生成和启动中的全部要求都能得到满足。

6.4.3 开发

6.4.3.1 功能规范

a) 评估方法

1) **审查产品的开发文档，查看是否具有功能规范设计文档；**

2) **审查功能规范设计文档，确认其是否描述了产品的所有安全功能和外部接口，是否包括所有外部安全功能接口的使用方法和用途，是否是内在一致的，是否能完备的表示产品安全功能。**

b) 预期结果

审查记录以及最后结果(符合/不符合)符合评估方法要求，开发者提供的文档内容应精确和完整。

6.4.3.2 高层设计

a) 评估方法

1) **审查产品的开发文档，查看是否具有高层设计文档；**

2) **审查高层设计文档，确认其是否按照子系统来描述产品安全功能的结构，是否描述了每个产品安全功能子系统所提供的安全功能性，是否标识了安全功能子系统的所有接口，是否标识了产品安全功能子系统的哪些接口是外部可见的，是否标识了产品安全功能所要求的任何基础性的硬件、固件或软件，以及在这些硬件、固件或软件中实现的支持性保护机制提供功能的一个表示，是否描述产品安全功能子系统所有接口的用途与使用方法，是否把产品分成安全策略实施和其他子系统来描述，是否以非形式化方式进行描述，是否是内在一致的。**

b) 预期结果

审查记录以及最后结果(符合/不符合)符合评估方法要求，开发者提供的高层设计内容应精确和完整。

6.4.4 指导性文档

6.4.4.1 管理员指南

a) 评估方法

1) 评价者应审查开发者是否提供了供授权管理员使用的管理员指南，并且此管理员指南是否包括如下内容：

——产品可以使用的管理功能和接口；

——怎样安全地管理产品；

——在安全处理环境中应进行控制的功能和权限；

——所有对与产品的安全操作有关的用户行为的假设；

——所有受管理员控制的安全参数，如果可能，应指明安全值；

——每一种与管理功能有关的安全相关事件，包括对安全功能所控制的实体的安全特性进行的改变；

——所有与授权管理员有关的 IT 环境的安全要求。

2) 审查产品的管理员指南，验证其是否与供评估的所有其他文档保持一致。

b) 预期结果

审查记录以及最后结果(符合/不符合)符合评估方法要求，开发者提供的管理员指南应完整。

6.4.4.2 用户指南

a) 评估方法

1) 评价者应审查开发者是否提供了供系统用户使用的用户指南，并且此用户指南是否包括如下内容：

——产品的非管理用户可使用的安全功能和接口；

——产品提供给用户的安全功能和接口的用法；

——用户可获取但应受安全处理环境控制的所有功能和权限；

——产品安全操作中用户所应承担的职责；

——与用户有关的 IT 环境的所有安全要求。

2) 审查产品的用户指南，验证其是否与供评估的所有其他文档保持一致。

b) 预期结果

测试记录以及最后结果(符合/不符合)符合评估方法要求，开发者提供的用户指南应完整。

6.4.5 测试

6.4.5.1 测试覆盖

a) 评估方法

审查开发者提供的测试覆盖分析，验证该分析是否证实了测试文档中所标识的测试和功能规范中所描述的安全功能是对应的，**验证功能规范中所描述安全功能和测试文档所标识的测试之间的对应性是否完备。**

b) 预期结果

测试覆盖中的全部要求都能得到满足。

6.4.5.2 功能测试

a) 评估方法

1) 审查测试文档是否包括测试计划、测试程序描述、预期测试结果和实际测试结果。

2) 审查测试计划是否标识了要测试的安全功能，描述了要执行的测试目标。

3) 审查测试程序描述是否标识了要执行的测试，并描述了每个安全功能的测试脚本。这些脚本包括对于其他测试结果的任意顺序依赖性。

4) 审查预期的测试结果是否与测试成功执行后的预期输出一致。

5) 审查文档中记录的预期测试结果和实际测试结果，确认每个被测试的安全性功能都按照规定运转。

b) 预期结果

审查记录以及最后结果(符合/不符合)符合评估方法要求，开发者提供的内容应完整。

6.4.5.3 独立性测试

a) 评估方法

1) 审查开发者提供的测试系统，提供的测试集合是否与其自测系统功能时使用的测试集合相一致。

2) 审查开发者是否提供一组相当的资源，用于安全功能的抽样测试。

b) 预期结果

审查记录以及最后结果(符合/不符合)符合评估方法要求。

6.4.6 脆弱性评定

6.4.6.1 脆弱性分析

a) 评估方法

1) 检查产品是否提供了脆弱性分析文档。

2) 审查脆弱性文档是否描述为搜索用户能违反产品安全策略的明显方法而执行的产品可交付材料分析。

3) 审查脆弱性文档,确认是否描述了明显的脆弱性的处置方法。

4) 审查脆弱性文档,确认是否针对所有已标识的脆弱性,说明了脆弱性不能在产品的预期使用环境中被利用。

b) 预期结果

审查记录以及最后结果(符合/不符合)符合评估方法要求,开发者提供的脆弱性分析文档应完整。

附 录 A
（资料性附录）
性能测试

A.1 性能指标

A.1.1 识别率

反垃圾邮件产品对垃圾邮件能够予以正确识别的比率。识别率＝(正确识别出的垃圾邮件数量/垃圾邮件的总数量)×100%。产品的技术文档应说明该产品的垃圾邮件识别率，并指明相应的测试环境、测试方法和测试工具。

A.1.2 误判率

反垃圾邮件产品把正常邮件判断为垃圾邮件的比率。误判率＝(错误报警为垃圾邮件的正常邮件数量/正常邮件的总数量)×100%。产品的技术文档应说明该产品的垃圾邮件误判率，并指明相应的测试环境、测试方法和测试工具。

A.2 性能测试

A.2.1 识别率

a) 测试评价方法

1) 在测试工具集中编辑测试邮件样本库，包括垃圾邮件和非垃圾邮件；
2) 在邮件服务器端配置若干接收邮件的帐户，由邮件客户端随机选取垃圾样本邮件发送，每次选取的样本数应不少于 100 份；
3) 记录反垃圾邮件产品对垃圾邮件的识别数量；
4) 重复以上过程 3 次。

b) 测试评价结果

反垃圾邮件产品应能报告检测到相应的垃圾邮件，计算产品所正确识别到的垃圾邮件数量和所发送垃圾邮件数量的比值，并取 3 次测试结果的平均值。

A.2.2 误判率

a) 测试评价方法

1) 在测试工具集中准备测试邮件样本库，包括垃圾邮件和非垃圾邮件；
2) 在邮件服务器端配置若干接收邮件的账户，由邮件客户端随机选取非垃圾样本邮件发送，每次选取的样本数应不少于 100 份；
3) 记录产品将非垃圾邮件识别为垃圾邮件的数量；
4) 重复以上过程 3 次。

b) 测试评价结果

反垃圾邮件产品对非垃圾邮件应该直接放行通过，计算产品误判为垃圾邮件的数量和所发送正常邮件数量的比值，并取 3 次测试结果的平均值。

参 考 文 献

[1] 公安部计算机信息系统安全产品质量监督检验中心.信息安全技术 反垃圾邮件产品检验规范.2006.

[2] 中国互联网协会.中国互联网协会反垃圾邮件规范.2004.

中 华 人 民 共 和 国
国 家 标 准
信息安全技术
反垃圾邮件产品技术要求和测试评价方法
GB/T 30282—2013
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲 2 号(100029)
北京市西城区三里河北街 16 号(100045)
网址:www.gb168.cn
服务热线:400-168-0010
010-68522006
2014 年 5 月第一版
*
书号:155066·1-48992

GB/T 30282-2013