

备案号: CNCA/CTS 0031-2008

信息安全产品认证技术规范

ISCCC TS004-2008

信息安全技术 反垃圾邮件产品认证技术规范

Information Security technology
Technical specifications for Anti-Spam product Certification

2008-10-08 发布

2008-10-08 实施

中国信息安全认证中心 发布

目 次

前 言	I
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 功能要求	2
4.1 静态黑白名单	2
4.2 实时黑名单	2
4.3 虚假路由邮件限制	2
4.4 邮件过滤	2
4.5 邮件处理	3
5 自身安全要求	3
5.1 安全审计	3
5.2 身份鉴别	4
5.3 用户角色	4
5.4 远程会话保护	4
6 性能要求	4
6.1 识别率	4
6.2 误报率	4
7 安全保证要求	4
7.1 配置管理	4
7.2 交付与运行	5
7.3 开发	5
7.4 指导性文档	6
7.5 测试	6
7.6 脆弱性评定	7
8 测评方法	7
8.1 测试环境与工具	7
8.2 功能测试	8
8.3 自身安全测试	11
8.4 性能测试	13
8.5 安全保证测试	14
参考文献	17

前 言

本技术规范是反垃圾邮件产品认证技术规范。

本技术规范由中国信息安全认证中心（ISCCC）提出并归口。

本技术规范起草单位：中国信息安全认证中心、上海市信息安全测评认证中心。

反垃圾邮件产品认证技术规范

1 范围

本技术规范规定了反垃圾邮件产品的技术要求。

本技术规范适用于第三方测评机构对反垃圾邮件产品的检测。反垃圾邮件产品的设计和实现也可参照使用。

2 规范性引用文件

下列文件中的有关条款通过引用而成为本技术规范的条款。凡注日期或版次的引用文件，其后的任何修改单（不包括勘误的内容）或修订版本都不适用于本技术规范，但提倡使用本技术规范的各方探讨使用其最新版本的可能性。凡不注日期或版次的引用文件，其最新版本适用于本技术规范。

GB/T 5271.8—2001 信息技术 词汇 第8部分：安全（idt ISO 2382-8:1998）

GB/T18336.1 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（idt ISO/IEC 15408-1:1999）

GB/T18336.3 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（idt ISO/IEC 15408-3:1999）

3 术语和定义

GB/T 5271.8—2001和GB/T 18336.1-2001确立的以及下列术语和定义适用于本技术规范。

下列术语和定义适用于本技术规范。

3.1

垃圾邮件 spam

是指包括下述属性的电子邮件：

— 收件人事先没有提出要求或者同意接收的广告、电子刊物、各种形式的宣传品等宣传性的电子邮件。

— 收件人无法拒收的电子邮件。

— 隐藏发件人身份、地址、标题等信息的电子邮件。

— 含有虚假的信息源、发件人、路由等信息的电子邮件。

3.2

实时黑名单 realtime black list

由权威机构和组织收集并维护的经常发送垃圾电子邮件的服务器地址列表。

3.3

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。

3.4

识别率 correct recognition rate

是指被保护的邮件服务器受到垃圾邮件攻击时，系统能够正确报警的概率。

识别率=正确报警的数量/垃圾邮件的数量

3.5

误报率 false position rate

是指系统把正常邮件判断为垃圾邮件而错误报警的概率。

误报率=错误报警的数量/正常邮件的数量

4 功能要求

4.1 静态黑白名单

反垃圾邮件产品

- a) 应提供静态黑名单功能。凡在黑名单中的邮件地址，产品直接拒绝连接而无需进行垃圾邮件判断工作。
- b) 可提供白名单的功能。凡在白名单中的邮件地址，产品将允许其正常通过而无需进行垃圾邮件检测。
- c) 应提供黑白名单的编辑（添加、删除等）功能，也可导入导出黑白名单。
- d) 黑白名单采取IP地址或邮件地址的形式。

4.2 实时黑名单

反垃圾邮件产品应

- a) 支持实时黑名单功能，通过DNS（Domain Name Server，域名服务器）查询方式来查询黑名单列表。
- b) 支持国家主管部门提供的实时黑名单服务。

4.3 虚假路由邮件限制

反垃圾邮件产品应能识别电子邮件的虚假路由，以确保用户的域名和IP地址相符；如果不符，则阻止邮件发送。

4.4 邮件过滤

反垃圾邮件产品应采取以下一种或几种邮件过滤规则实现其反垃圾邮件功能。

4.4.1 邮件发送地址过滤

反垃圾邮件产品应能对发送电子邮件的特定网络地址进行阻断。

4.4.2 邮件静态特征过滤

反垃圾邮件产品应支持以下静态特征过滤规则：

- a) 关键字过滤：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、邮件附件名中包含的设定关键字。
- b) 数值过滤：根据邮件或附件的尺寸、附件的数量、收件人总数等数值特征进行匹配限制。
- c) 附件过滤：根据附件的文件名和附件类型等特征进行过滤。
- d) 或基于其它特征进行过滤。

多个过滤规则可以按“与”、“或”、“非”的逻辑关系组合成更为复杂的过滤条件。

4.4.3 邮件行为特征限制

反垃圾邮件产品应能限制：

- a) 同一IP地址对邮件服务端口的最大同时TCP（Transmission Control Protocol，传输控制协议）和SMTP（Simple Mail Transfer Protocol，简单邮件传输协议）连接数量。
- b) 一段时间内同一IP地址对邮件服务端口的最大TCP和SMTP连接次数。
- c) 一段时间内同一主题的邮件接收次数。

当超过该连接数目时，系统能够自动阻止新的连接。或基于其它连接特征识别出异常时，能自动进行阻断。

4.5 邮件处理

反垃圾邮件产品对垃圾邮件应提供以下处理方式：

- a) 投递。不对邮件进行任何处理，直接放行。
- b) 标记投递。在邮件中将邮件标记为垃圾邮件后通知或投递给收件人。
- c) 隔离。邮件放入专门隔离区中，供授权管理员进一步处理，暂不投递给收件人。
- d) 拒绝。拒绝接收邮件，并通知发件人邮件被拒收。
- e) 丢弃。将邮件直接丢弃而不通知发件人。

5 自身安全要求

5.1 安全审计

5.1.1 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，导致的会话连接终止。
- 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。

5.1.2 审计数据管理

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。
- 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 身份鉴别

反垃圾邮件产品应：

- a) 对授权管理员进行身份鉴别，且身份鉴别方式（如用户名+口令）应有一定的强度保证。
- b) 限制登录失败次数，并有鉴别失败的处理措施，如限定登录IP地址、列入禁止访问列表等。

5.3 用户角色

反垃圾邮件产品应定义不同的管理角色，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。

5.4 远程会话保护

如果反垃圾邮件产品支持远程WEB管理，应采取安全措施来保护远程管理会话。

6 性能要求

6.1 识别率

应维持一定水平的识别率，不能对正常使用产品产生较大影响。

6.2 误报率

应将误报率控制在应用许可的范围，不能对正常使用产品产生较大影响。

7 安全保证要求

7.1 配置管理

7.1.1 配置管理能力

- a) 开发者应使用配置管理系统并提供配置管理文档，以及为产品的不同版本提供唯一的标识。
- b) 配置管理系统应对所有的配置项作出唯一的标识，并保证只有经过授权才能修改配置项。
- c) 配置管理文档应包括配置清单和配置管理计划。在配置清单中，应对每一配置项给出相应的描述。在配置管理计划中，应描述配置管理系统是如何使用的。实施的配置管理应与配置管理计划相一致。
- d) 配置管理文档还应描述对配置项给出唯一标识的方法，并提供所有的配置项得到有效地维护的证据。

7.2 交付与运行

7.2.1 交付

- a) 开发者应使用一定的交付程序交付产品，并将交付过程文档化。
- b) 交付文档应描述在给用户方交付产品的各版本时，为维护安全所必需的所有程序。

7.2.2 安装、生成和启动

开发者应提供文档说明产品的安装、生成和启动的过程。

7.3 开发

7.3.1 非形式化功能规范

开发者应提供功能规范，该功能规范：

- a) 应使用非形式化语言来描述产品的安全功能及其外部接口。
- b) 应内在一致。
- c) 应描述所有外部安全功能接口的用途与使用方法，适当的时候要提供影响、例外情况和错误消息的细节。
- d) 应完整地表示产品的安全功能。

7.3.2 描述性高层设计

开发者应提供产品安全功能的高层设计，该高层设计应

- a) 以非形式化来表示。
- b) 保持内在一致。
- c) 按子系统来描述产品的安全功能结构。
- d) 描述安全功能的每一个子系统所提供的安全功能。
- e) 标识安全功能所要求的任何基础性硬件、固件或软件。

- f) 标识安全功能子系统的的所有接口。
- g) 标识安全功能子系统的哪些接口是外部可见的。

7.4 指导性文档

7.4.1 管理员指南

开发者应提供管理员指南。管理员指南应描述：

- a) 管理员可使用的管理功能和接口。
- b) 怎样以安全的方式管理产品。
- c) 在安全处理环境中应进行控制的功能和权限。
- d) 所有对与产品的安全操作有关的用户行为的假设。
- e) 所有受管理员控制的安全参数，如果可能，应指明安全值。
- f) 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。
- g) 所有与管理员有关的IT环境的安全要求。

管理员指南应与为评估而提供的其他所有文档保持一致。

7.4.2 用户指南

开发者应提供用户指南。用户指南应描述：

- a) 非管理员用户可使用的功能和接口。
- b) 使用产品提供的的安全功能和接口的用法。
- c) 用户可获取但应受安全处理环境控制的所有功能和权限。
- d) 产品安全运行中用户所应承担的职责。
- e) 与用户有关的IT环境的所有安全要求。

用户指南应与为评估而提供的其他所有文档保持一致。

7.5 测试

7.5.1 范围

开发者应提供测试覆盖范围的分析结果，该分析结果应表明测试文档中所标识的测试与安全功能设计中所描述的安全功能是对应的，且该对应是完整的。

7.5.2 功能测试

- a) 开发者应测试产品的功能，并记录结果。

- b) 开发者应提供测试文档。
- c) 测试文档应包括测试计划、测试过程描述、预期的测试结果和实际测试结果。
- d) 测试文档应标识将要测试的产品功能，并描述将要达到的测试目标。
- e) 测试过程描述应标识要执行的测试，并描述每个安全功能的测试概况，这些概况包括对其它测试结果的顺序依赖性。
- f) 开发者的期望测试结果应表明测试成功后的预期输出。实际测试结果应表明每个被测试的安全功能能按照规定进行运作。

7.6 脆弱性评定

7.6.1 指南检查

开发者应提供文档。在文档中应确定对产品的所有可能的操作方式（包含失败和操作失误后的操作）、它们的后果以及对于保持安全操作的意义。文档中还应列出所有目标环境的假设以及所有外部安全措施（包含外部程序的、物理的或人员的控制）的要求。文档应是完整的、清晰的、一致的、合理的。

7.6.2 脆弱性分析

- a) 开发者应从用户可能破坏安全策略的明显途径出发，对产品的各种功能进行分析并提供文档。对被确定的脆弱性，开发者应明确记录采取的措施。
- b) 对每一条脆弱性，应有证据显示在使用产品的环境中该脆弱性不能被利用。

8 测评方法

8.1 测试环境与工具

反垃圾邮件产品安全功能测试和性能测试的典型测试环境分别如图1和图2所示。

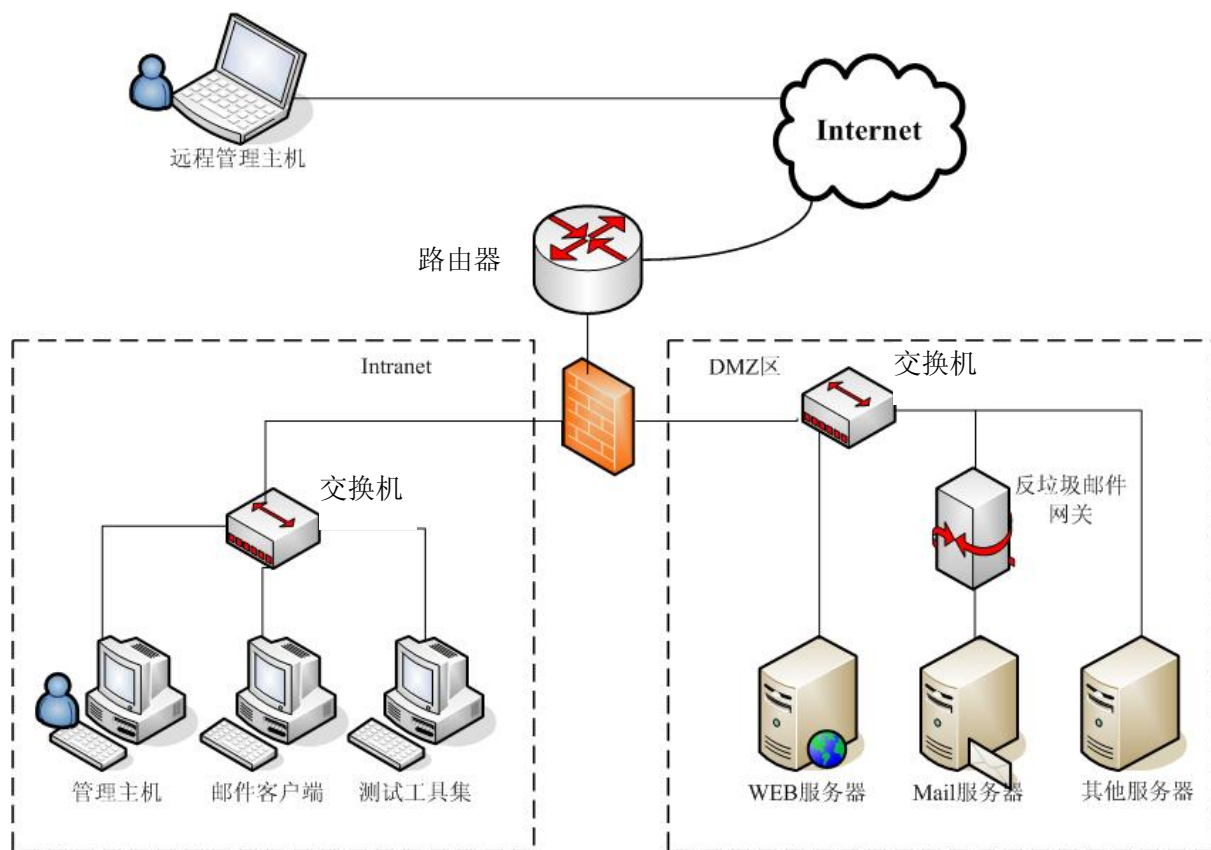


图1 反垃圾邮件产品安全功能测试环境图

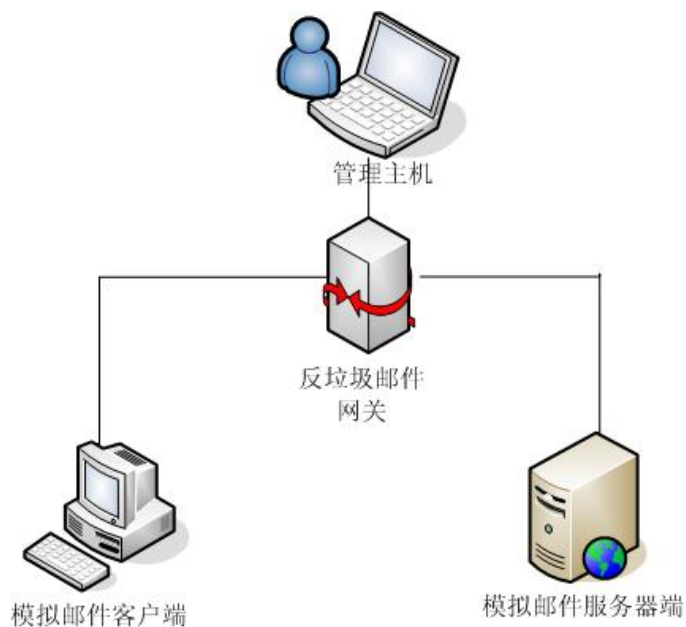


图2 反垃圾邮件产品性能测试环境图

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：能够模拟邮件客户端和邮件服务器端的专用网络性能分析仪器进行邮件的发送和接收。能够进行邮件群发的的测试工具集等。

8.2 功能测试

8.2.1 静态黑白名单

- a) 测试评价方法
 - 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) 配置白名单列表，并验证白名单设置的有效性。
 - 3) 手工添加、删除黑白名单，导入导出黑白名单，检查产品是否具有黑白名单编辑功能。
 - 4) 检查黑白名单的形式。
- b) 测试评价结果
 - 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) 产品不对白名单用户发送的邮件进行垃圾邮件判断，邮件直接发送到接收客户端。
 - 3) 可以手工编辑黑白名单，并可将文件导入导出黑白名单。
 - 4) 黑白名单采取 IP 地址或邮件地址的形式。

8.2.2 实时黑名单

- a) 测试评价方法
 - 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) 测试评价结果
 - 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) 支持国内主管部门提供的实时黑名单列表。
 - 3) 对实时黑名单列表中用户发送的邮件进行阻断。

8.2.3 虚假路由邮件限制

- a) 测试评价方法
 - 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) 测试评价结果
 - 反垃圾邮件产品能识别并阻断虚假路由邮件的发送。

8.2.4 邮件过滤

8.2.4.1 邮件发送地址过滤

a) 测试评价方法

- 1) 设定邮件客户端IP为需阻断地特定网络地址，由邮件客户端向Mail服务器端发送邮件，验证产品对所设定地址的阻断功能。
- 2) 启用实时黑名单功能，审查产品说明书分析产品是否支持连接多个可用的实时黑名单服务网站，可阻断常用垃圾邮件服务器地址。

b) 测试评价结果

- 1) 产品能根据限定IP地址对邮件发送方发送的邮件进行阻断。
- 2) 产品支持多个实时黑名单服务器网站，能够阻断常见的垃圾邮件服务器。

8.2.4.2 邮件静态特征过滤

a) 测试评价方法

- 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、邮件附件名设定不同的关键字，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、收件人总数等特征阈值，自邮件客户端向邮件服务器发送超过设定阈值的邮件。
- 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) 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。
- 5) 分别判断产品是否能对上述邮件进行过滤。
- 6) 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) 测试评价结果

反垃圾邮件产品能根据邮件的关键字、邮件数值特征和附件特征及其组合条件对邮件进行扫描过滤。

8.2.4.3 邮件行为特征限制

a) 测试评价方法

- 1) 设定测试工具集IP对邮件服务器的最大同时SMTP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) 设定测试工具集IP对邮件服务器的一段时间内的最大SMTP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) 测试评价结果
- 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。

8.2.5 邮件处理

- a) 测试评价方法
- 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，验证产品对垃圾邮件的处理结果。
- b) 测试评价结果
- 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。

8.3 自身安全测试

8.3.1 安全审计

8.3.1.1 审计数据生成

- a) 测试评价方法
- 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产品，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) 测试评价结果
- 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。

8.3.1.2 审计数据管理

a) 测试评价方法

- 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) 测试评价结果

- 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（图）。

8.3.2 身份鉴别

a) 测试评价方法

- 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) 测试评价结果

- 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，应采取相应措施，并生成审计记录。
- 5) 最大失败次数仅由授权管理员设定。

8.3.3 用户角色

a) 测试评价方法

- 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权限划分，内容过滤策略和黑白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) 测试评价结果

- 1) 产品允许定义多个角色的用户。

- 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) 每一个用户标识是唯一的，不应一个用户标识用于多个用户。

8.3.4 远程会话保护

- a) 测试评价方法：审查产品说明手册，当产品需要通过网络进行远程管理时，是否能提供对管理信息进行安全传输的功能。
- b) 测试评价结果：记录审查结果并对该结果是否符合测试评价方法要求作出判断。当产品需要通过网络进行远程管理时，产品应能对管理信息进行保密传输。

8.4 性能测试

8.4.1 识别率

- a) 测试评价方法
 - 1) 准备测试邮件样本库，包括大量垃圾邮件和少量非垃圾邮件。
 - 2) 在模拟邮件服务器端配置若干接收邮件的帐户，由模拟邮件客户端随机选取垃圾样本邮件发送。
 - 3) 记录产品对垃圾邮件的识别数量。
 - 4) 重复以上过程三次。
- 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，并取三次测试结果的平均值。

8.4.2 误报率

- a) 测试评价方法
 - 1) 准备测试邮件样本库，包括少量垃圾邮件和大量非垃圾邮件。
 - 2) 在模拟邮件服务器端配置若干接收邮件的帐户，由模拟邮件客户端随机选取非垃圾样本邮件发送。
 - 3) 记录产品将非垃圾邮件识别为垃圾邮件的数量。
 - 4) 重复以上过程三次。
- 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非垃圾邮件数量的比值，并取三次测试结果的平均值。

8.5 安全保证测试

8.5.1 配置管理

a) 测试评价方法

评估者应审查开发者所提供的信息是否满足7.1.1中的要求。

b) 测试评价结果

记录审查结果并对该结果是否符合测试要求作出判断。开发者提供的配置管理内容应完整。

8.5.2 交付与运行

8.5.2.1 交付

a) 测试评价方法

评估者应审查开发者是否使用一定的交付程序交付产品，并使用物理文档描述交付过程，并且评估者应审查开发者交付的文档是否包含以下内容：在给用户方交付产品的各版本时，为维护安全所必需的所有程序。

b) 测试评价结果

记录审查结果并对该结果是否符合测试评价方法要求作出判断，开发者应提供完整的文档描述所有交付的过程。

8.5.2.2 安装、生成和启动

a) 测试评价方法

评估者应审查开发者是否提供了文档说明产品的安装、生成和启动的过程。用户能够通过此文档了解安装、生成和启动过程。

b) 测试评价结果

记录审查结果并对该结果是否符合测试评价方法要求作出判断。

8.5.3 开发

8.5.3.1 非形式化功能规范

a) 测试评价方法

评估者应审查开发者提供的信息满足7.3.1中有关内容和形式的所有要求。

b) 测试评价结果

记录审查结果并对该结果是否符合测试要求作出判断。

8.5.3.2 描述性高层设计

a) 测试评价方法

评估者应审查开发者提供的信息满足7.3.2中有关内容和形式的所有要求。

b) 测试评价结果

记录审查结果并对该结果是否符合测试要求作出判断。

8.5.4 指导性文档

8.5.4.1 管理员指南

a) 测试评价方法

评估者应审查开发者是否提供了供管理员使用的管理员指南，并且此管理员指南是否包含7.4.1中所描述的内容。

b) 测试评价结果

记录审查结果并对该结果是否符合测试评价方法要求作出判断，评估者审查内容至少包含测试要求中所列的内容。

8.5.4.2 用户指南

a) 测试评价方法

评估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含7.4.2中所描述的内容；审查用户指南是否与为评价而提供的其他所有文件保持一致。

b) 测试评价结果

记录审查结果并对该结果是否符合测试评价方法要求作出判断，评估者审查内容至少包含测试要求中所列的内容。

8.5.5 测试

8.5.5.1 范围

a) 测试评价方法

评估者应审查开发者提供的测试覆盖范围分析结果，是否表明了测试文档中所标识的测试与安全功能设计中所描述的安全功能是对应的；评价测试文档中所标识的测试是否完整。

b) 测试评价结果

记录审查结果并对该结果是否符合测试评价方法要求作出判断。

8.5.5.2 功能测试

a) 测试评价方法

- 1) 评价开发者提供的测试文档，是否包含测试计划、测试过程描述和测试结果。
- 2) 评价测试文档是否标识了将要测试的产品功能，是否描述了将要达到的测试目标。
- 3) 评价测试过程是否标识了要执行的测试，是否描述了每个安全功能的测试情况（包括对其它测试结果的顺序依赖性）。
- 4) 评价测试文档的测试结果是否给出全部测试的测试评价结果。
- 5) 评价实际测试结果是否表明每个被测试的安全功能能按照规定进行运作。

b) 测试评价结果

记录审查结果并对该结果是否符合测试评价方法要求作出判断，评估者审查内容至少包含测试评价方法中的五方面。开发者提供的内容应完整。

8.5.6 脆弱性分析

8.5.6.1 指南检查

a) 测试评价方法：

评估者应确认开发者提供的文档是否满足了以下要求：

- 1) 是否确定对产品的所有可能的操作方式（包含失败和操作失误后的操作），是否确定它们的后果，以及是否确定对于保持安全操作的意义。
- 2) 是否列出所有目标环境的假设以及所有外部安全措施（包含外部程序的、物理的或人员的控制）的要求。
- 3) 是否完整、清晰、一致、合理。

b) 测试评价结果

记录审查结果并对该结果是否符合测试评价方法要求作出判断。

8.5.6.2 脆弱性分析

a) 测试评价方法

- 1) 评估开发者提供的脆弱性分析文档，是否从用户可能破坏安全策略的明显途径出发，对产品的各种功能进行分析。
- 2) 对被确定的脆弱性，评估开发者是否明确记录了采取的措施。
- 3) 对每一条脆弱性，评估是否有证据显示在使用产品的环境中该脆弱性不能被利用。

b) 测试评价结果

记录审查结果并对该结果是否符合测试评价方法要求作出判断，开发者提供的脆弱性分析文档应完整。

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] 陈勇, 李卓桓. 反垃圾邮件完全手册. 清华大学出版社. 2006
- [3] 中国互联网协会. 《中国互联网协会反垃圾邮件规范》2004. 2. 26
- [4] GB/T18336. 2-2001 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
-