

金笛邮件系统反垃圾设置指南

一. 概述

邮件系统提供强大的，完备反垃圾功能。系统提供 smtp 服务层，和基于邮件内容分析的双层反垃圾功能。

二. Smtplib 服务反垃圾设置

通过 smtp 服务层把明显的发送垃圾邮件的 smtp 连接拒绝，大大减轻后台投递系统和反垃圾引擎的负载。

通过统计分析，我们发现很多发送垃圾邮件的 smtp 连接具有以下特点。

1. 同一 ip 同时的 smtp 连接数非常大。
 2. 同一 ip 在一段时间，smtp 连接频率非常大。
- 一般出现这两种情况，都表示源发件人非常有可能发送垃圾邮件。

通过设置以下这两个参数可控制这类型的 smtp 连接，从而截断发送垃圾邮件的源头：

1. 系统设置—SMTP 服务—一分钟同一 IP 允许访问次数
2. 系统设置—SMTP 服务—同一 IP 最大同时访问数

同时设置：

系统设置—SMTP 服务—启用智能反垃圾 IP 功能

参数，把符合以上两个条件的 ip 地址自动加入系统的智能反垃圾 IP 列表中（SmartSpamIP），当以后系统碰到这些 ip 的连接的时候，直接拒绝。

可通过：

系统监控—智能反垃圾IP列表

查看系统目前智能反垃圾IP 列表。

注意点：

当互联网是经过反垃圾网关再接入邮件系统的情况，由于邮件系统的所有 smtp 连接都来自反垃圾网关，所以基于 Smtplib 服务反垃圾不再起作用，这是需要把以上两个参数设为-1，以免系统 smtp 服务故障。

三. 反垃圾引擎设置

系统反垃圾引擎主要由以下四部分组成：

1. 基于 SpamAssassin 反垃圾功能

SpamAssassin 是一个由 Apache 开发的一个著名的反垃圾引擎，邮件系统完整的集成了 SpamAssassin 反垃圾引擎。

邮件系统提供了一个名为 SA-Server 的 SpamAssassin 反垃圾服务器，邮件系统通过把需要进行反垃圾分析的邮件提交给 SA-Server 进行分析。

SA-Server 在 Windows 平台上可通过 SA_Server 服务启动，在 Unix/Linux 平台上可通过 sa/sa_server.sh 脚本启动。

SA-Server 默认端口为 8700，可通过直接修改 sa/sa_server.pl 修改这个端口。

可通过邮件管理系统中的，反垃圾\反病毒—反垃圾引擎设置 中的 SpamAssassin 中的相关设置进行 SA-Server 的服务配置。

其中：

启用 SpamAssassin ， 指定是否启动 SpamAssassin 反垃圾检查

SpamAssassin 服务器地址，指定 SA-Server 服务器地址，默认为本机。

SpamAssassin 服务端口，指定 SA-Server 服务器端口，默认为 8700。

最大 SpamAssassin 检查线程数，指定最大的连接 SA-Server 服务数，可根据系统的复杂进行适当调整。

2. 邮件内容关键字，来源以及实时黑名单分析

垃圾邮件内容分析

通过邮件内容关键字分析，可为符合内容分析结果的邮件打上相应的垃圾邮件评分。这类规则的判断条件类似系统的过滤规则。

邮件来源分析

主要通过分析邮件的来源，如：发件人 ip，发件人，发件域，等内容，来判断垃圾邮件的可能性。

实时黑名单(RBL)

主要通过利用互联网公开的 rbl 资源判断垃圾邮件的可能性。目前 RBL 一般都通过 DNS 查询的方式提供对某个 IP 或域名是否是垃圾邮件发送源的判断。另外，由于国外大多数 rbl 都对来自中国的 ip 有“歧视”，所以我们并不能完全依靠 rbl 来判断一封邮件是否是垃圾邮件，只能根据 rbl 查询结果判断邮件是否垃圾邮件的可能性。可设置以下参数，定制 rbl:

| | |
|---|--|
| RBL 服务器地址 | <input type="text" value="xbl.spanhaus.org"/> |
| DNS 查询类型 | <input type="text" value="A"/> |
| 得分 | <input type="text" value="3.0"/> |
| 匹配表达式 | <input type="text" value="127\.\d+\.\d+\.[45]"/> |
| 描述 | <input type="text"/> |
| <input type="button" value="保存"/> <input type="button" value="取消"/> | |

RBL 服务器，指定 RBL 查询域名后缀。

DNS 查询类型，根据具体的 RBL 要求指定 DNS 查询记录类型。

匹配表达式，指定 RBL 查询结果的匹配模式，表达式格式采用 perl 正则表达式，如果为空，则表示如果可查到 RBL 结果，就表示符合条件。

3. 贝叶斯(Bayes)统计分析

贝叶斯分析：命名于著名数学家托马斯贝叶斯（1702-1761），他发展了一个数学领域全新的可能性推论理论。贝叶斯分析采用过去事件的知识预测未来事件。应用到反垃圾邮件领域，贝叶斯过滤与以前收到的垃圾邮件与合法邮件的中相同词语与短语出现的频率对比此邮件中有问题的词语与短语的来确定垃圾邮件的可能性。他能自动适应垃圾邮件变化。是一种动态的智能过滤技术。

要使用贝叶斯统计分析，必须要初始化贝叶斯数据库。根据具体需求收集适合系统的垃圾邮件和正常邮件词汇集，通过系统的“贝叶斯(Bayes)数据库初始化”功能进行贝叶斯数据初始化