爱思华宝统一通信

反垃圾向导

版本 10.4

目录

反垃圾 1

反垃圾 2

新的内部处理 2

总得分和垃圾杀手得分分离 2

智能通迅录自动白名单特性 2

新的垃圾邮件报告 2

分布式域 2

反垃圾 - 垃圾邮件计分 3

参考 4

常规 5

常规 5

其他 6

动作 10

动作 10

报告 12

如何设置反垃圾报告 13

不同的报告时间表 16

隔离 18

隔离 - 隔离报告 20

隔离 处理接收的邮件 22

隔离 - 处理队列中的邮件 23

挑战响应 - 如何工作 24

邮箱管理系统发给发送者的确认请求 25

待授权的发送者 在数据库中等待解决 25
发送者确认请求的网页 URL 26
发送者如输入正确代码，则自动被授权。 26
被授权的发送者将被添加至询问响应中。 26
反垃圾 - 垃圾杀手 27
RBL 29
爱思华宝在线反垃圾 30
爱思华宝在线反垃圾 分级 31
报告错误的分类 33
报告邮件地址 34
反垃圾 - 贝叶斯 36
贝叶斯过滤器 - 基本概念 37
反垃圾 - 黑白名单 39
黑名单 39
白名单 40
灰名单 42
灰名单流程图 43
反垃圾 - 学习规则 45
其他 47
内容 47
其他 - 字符集 48
发件人 48

反垃圾模板 50

规则自定义 -local.cf 文件 51

反垃圾 - 垃圾邮件队列 53

反垃圾 - 日志 54

原因码 56

反垃圾流程图 58

第 1 章

反垃圾

爱思华宝服务器结合了多种反垃圾邮件技术来防止垃圾邮件。

爱思华宝服务器采用垃圾杀手，贝叶斯过滤，灰名单，Razor 和内容过滤器等技术，让你拥有当今市场上最全面的反垃圾工具。

邮件是否被标记为垃圾邮件是基于计分标准的，满分为 10 分。最后由爱思华宝服务器检查这一邮件的计分，并采取相应动作。你设定的垃圾邮件计分规则可能会导致邮件被列为垃圾邮件，被隔离或被删除。

Legend

图标	描述
	警告 – 非常重要！
	便笺或提示 – 好的建议。
NOTE: Areas...	表内注意。
▸ Figure 4	图表链接 – 点击连接显示图例，再次点击将其关闭。 (只工作在 CHM 格式。)

本章内容

反垃圾 2
反垃圾 - 垃圾邮件计分.....3
向导 4
反垃圾模版 50
规则自定义 -local.cf 文件 51
反垃圾 - 垃圾邮件队列.....53
登陆 54
原因码 56
反垃圾流程图.....58

反垃圾

新的内部处理

重新设计和文档化。解决所有已知问题包括忽略缺陷，访问模式，多个收件人问题，内容过滤器冲突等等。

总得分和垃圾杀手得分分离

反垃圾总得分和垃圾杀手得分现在是二个单独的值，在日志和信头报告中被单独记录，以便分析和微调。

智能通迅录自动白名单特性

增强的伪造邮件保护，通过 邮件服务 - 安全 - 常规 - 安全 ?#25298;绝发件人域为本地去未经验证的邮件?选项。现在检查 From 和 From 信头，如果其中任何一个包含本地域，非验证的收件人，它会跳过所有的白名单和忽略(DB 白名单，IM 联系人白名单)。如果 **SpamSkipBypassLocalUntrusted** 选项(**spam.dat** ，默认情况下启用)正在运行，即使邮件应该隔离区白名单会跳过。

新的垃圾邮件报告

DB 驱动，新的隔离区 API ，新的脚本，自动引擎 URL ，单个用户/域/域别名支持，速度，性能和存储最佳化，处理数千帐户，增加日志。系统 URI 从 **/challenge/** 更新到 **/reports/** 。

分布式域

注意：对于分布式域里的外部收件人，反垃圾将不被执行，这可以通过 API 变量禁用 ***C_AS_BypassDistributedDomain*** (设置为 0)。如果禁用，对于 出站邮件 反垃圾将被执行。

学习规则 -- EML 支持

.eml 文件发送到学习规则帐户同样进行相应处理。

扩展日志

查看真实的收件人动作，多个邮件收件人将分别记录。

亚洲语系贝叶斯

处理中文邮件优化，**spam.dat** 中新选项，需要学习，亚洲语系垃圾杀手推荐。

反垃圾 - 垃圾邮件计分

首先你应该理解垃圾邮件计分的概念。

爱思华宝服务器利用多种反垃圾邮件技术检查和处理邮件，并能依据每次检查的结果更改邮件计分。

垃圾邮件计分的有效值是从 0 分到 10 分，以表明邮件成为垃圾邮件的可能性，分值达到了 10 分表明这一邮件极有可能是垃圾邮件。

爱思华宝服务器内部的一些设置允许您更改邮件的已有计分(例如- 内容检查)。爱思华宝服务器在此部分将为您的邮件计分增加你输入的设定值。因此，如果你在"计算没有标题，没有邮件主体的邮件的分值" 输入 1.5 分。如果测试结果为真，那么邮件计分将上升 1.5。

参考

本章描述爱思华宝服务器管理员控制台的 反垃圾 节点。

本章内容

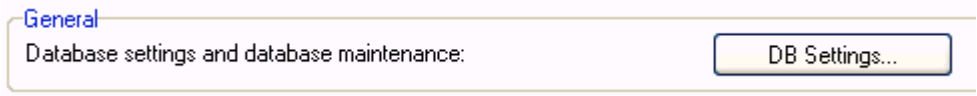
常规 5
动作 10
隔离 18
垃圾杀手 27
垃圾杀手-RBL 29
爱思华宝在线反垃圾.....30
贝叶斯 36
反垃圾 - 黑白名单 39
灰名单 42
学习规则 45
其他 47

常规

本章内容

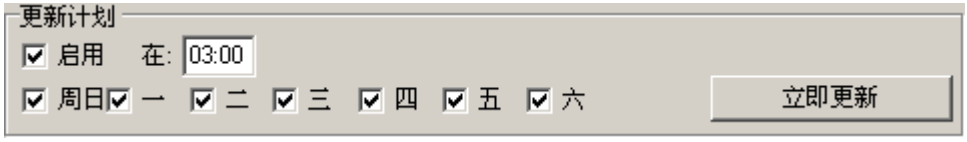
常规 5
其他 6

常规



字段	描述
数据库设置和维护	点击 DB 设置 **修改** 数据库设置。(更多详细内容请参考 数据库设置 部份。) 默认情况下，爱思华宝服务器上安装了一个 MS Access 数据库存储数据。你应当清楚，当这个数据库的记录超过 10k，Access 运行的速度将变得非常缓慢。因此，你应该考虑将数据转移到专业的数据库。

注意：该服务器的访问模式可以通过域和用户级别进行设置，请参考相应位置 ([域] -- 策略, [用户] --策略)。

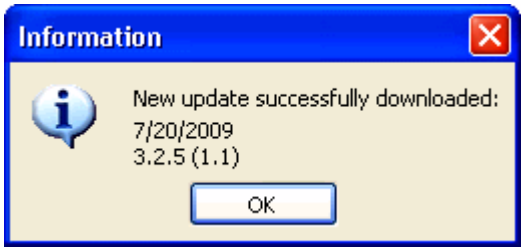


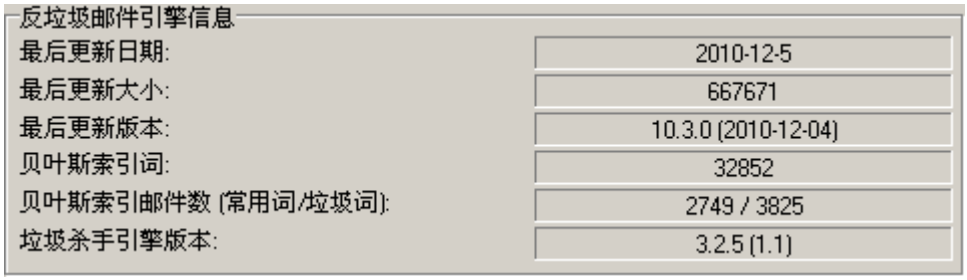
"更新计划" 部分允许爱思华宝服务器根据排程自动更新反垃圾邮件参考库，从而使贝叶斯过滤器准确识别垃圾邮件。

我们的员工将维护这一参考库，它能确保大多数用户最佳的贝叶斯过滤性能。解决数百万计的垃圾邮件,使用正常电子邮件的准确性近百分百。

注意：基于服务器的索引（详见 **反垃圾贝叶斯**) 将创建一个独立的用户参考库。

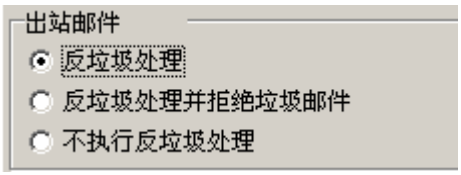
字段	描述
启用	勾选本项使基本数据库能够自动更新。
在:	指定更新的时间。

周日 - 周六	检查更新的时间段。
立即更新	如果需要，点击 **立即更新** 按钮立即更新反垃圾引擎。 如果没有问题，你将看到一个与下面类似的信息框。 



字段	**描述**
最后更新日期	反垃圾邮件引擎的最后更新日期。
最后更新大小	显示最后更新文件的容量。 可用于故障检查。
最后更新版本	使用中的引擎版本。
贝叶斯索引词	显示贝叶斯数据库中的索引词数目。
贝叶斯索引比例(常用词/垃圾词)	分析显示的正常和垃圾邮件信息数目，得出贝叶斯数据库。
垃圾杀手版本	运行中的垃圾杀手引擎版本。

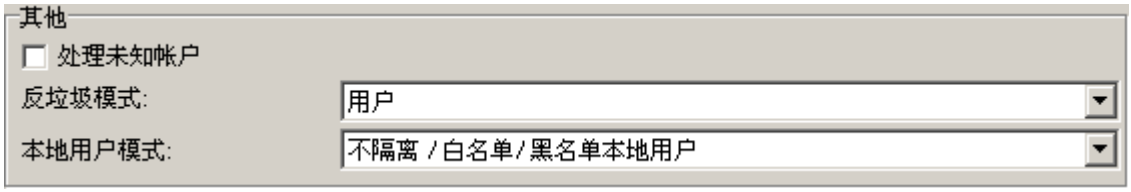
其他



上述选项用于指定出站邮件的反垃圾处理方式。

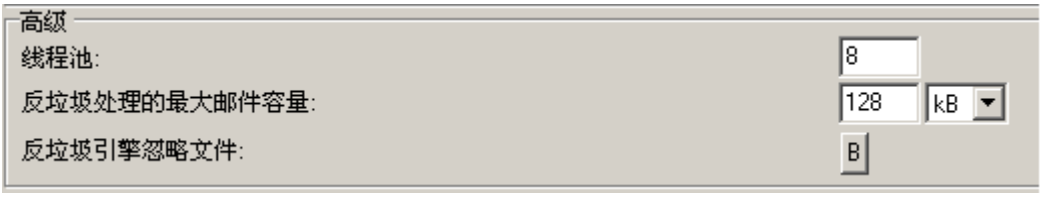
选择列表选项：

字段	描述
反垃圾处理	此选项用于处理所有邮件并进行转发，而不管处理结果如何。 根据你的设置，被判为垃圾的邮件会被标记后再发送。
反垃圾处理并拒绝垃圾邮件	此选项用于处理所有邮件，拒绝任何被识别为垃圾邮件的信息。
不执行反垃圾处理	使用此选项跳过反垃圾邮件处理。 只有在信任系统上的所有用户时，才能选择此选项。



字段	描述
处理未知帐户	本选项告诉爱思华宝服务器反垃圾引擎如何处理一封来自未定义帐户的邮件(例如一封入站邮件通过规则被转发到一个指定帐户)。 勾选本项则邮件将被反垃圾引擎处理。
反垃圾模式	从以下选项中选择： **用户** 邮件地址将被添加到收件人的白名单。 该模式适合于 ISP，因为他们的域内帐户彼此无关。 **域** 邮件地址被添加到收件人域的白名单。 这种模式适合于拥有多个 "公司" 域的 ISP，所有域用户都与某个域有关。 **系统** 邮件地址被添加到整个爱思华宝服务器的白名单。 该模式适用于企业的爱思华宝服务器。 注意：设置反垃圾模式为域或系统会使黑名单和白名单记录显示难于理解，比如有些指定用户帐户作为记录的所有者，这会导致一些混乱如其他用户质疑为什么一封邮件会通过或被拦截。 注意：同样我们也不推荐经常改变模式，如必须改变时请记录该将改变的情况，以便在黑白名单处理混乱时能追查到具体的原因。 注意:当 **可信的邮件收件人自动列入白名单数据库** 选项被启用时，本功能可能带来一些数据库级的影响.

	更多关于白名单、自动白名单以及白名单清除的详细信息，请参考 ***反垃圾 -- 白名单*** 章节。
本地用户模式	从以下三选项中选择一个处理来自同一服务器的不同用户邮件的方式(但可能在不同的域)。 **不隔离/ 白名单/ 黑名单本地用户** 来自本服务器的域用户将不被检查。 使用本选项你将信任本地服务器中所有域的用户。 **隔离/ 白名单/ 黑名单所有本地用户** 所有用户都将被检查。 使用该选项你主机中所有的域和用户彼此间不相互信任。 **隔离/ 白名单/ 黑名单来自其他域的用户** 来自于服务器上不同域的用户将被检查。 使用本选项你主机上的本域用户会被信任，但不同域的用户不被信任。



字段	描述
线程池	定义反垃圾引擎用于处理邮件的最大线程数。 这一方法能有效的减轻（或增加）服务器的负载。
反垃圾处理的最大邮件容量	设定反垃圾引擎所能处理的最大邮件，大于该容量的邮件将不被处理。
反垃圾引擎忽略文件	按下按钮打开 忽略 文件，列表中的所有用户、帐户或域发送的邮件都将不被反垃圾引擎处理， 忽略 对话框将打开。更多关于该对话框的信息，请参考 忽略 规则/过滤器 部份。

注意：您可以通过在设置文件中设置一个文件名来获得垃圾杀手的规则状态。 要实现这些请在设置文件中添加 ***spamassassinrulestats*** 条目：

spamassassinrulestats="<filename>"

如果你想创建每日/每小时的文件等这里你可以使用日期/时间变量。

spamassassinrulestats="yyyymmddhhnnss.txt"

该文件的内容将让您了解哪些规则已经使用和规则的设置情况。截取其中简单的一段作为例子：

```
SpamAssassin statistics 2007-08-15 00:00
```

```
  Genuine: 649
  SpamQuarantine: 0
  SpamMarked: 416
  SpamRefused: 205
  SpamAssassin: 481
  Rules: 1293
  Hits: 254
  TotalHits: 13588
  NoHits: 1039

  Rules with hits:
  __FRAUD_DBI (1.00) 29
  .... list of rules
  Total: 254, Hits: 13588

  Rules with no hits:
  DRUGS_DEPR_EREC (1.00) # Refers to both an erectile and an antidepressant ... list of
     rules
Total: 1039
```

动作

本章内容

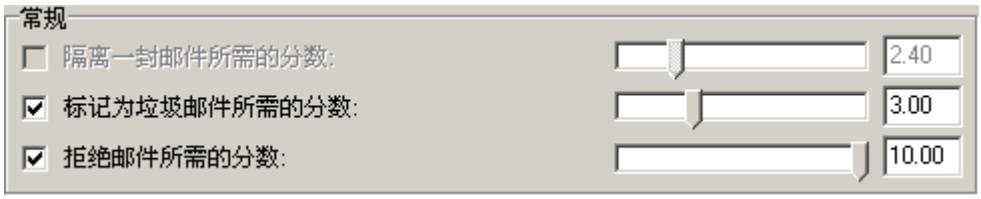
动作 10
报告 12

动作

动作 选项卡允许你定义不同垃圾得分时所采取的动作。

应注意的是，垃圾邮件分数在 0 与 10 之间，若分数为 10，则表示此邮件为垃圾邮件的可能性最高。

如果邮件被设定为不被反垃圾处理，那么它的得分将为 0。



字段	描述
隔离一封邮件所需要的分数	若邮件分数等于或高于所选值，则邮件将被隔离。 可移动滑动块对分数进行更改。 注意 首先必须激活 **隔离** 功能才可用。
标记为垃圾邮件所需的分数	若邮件分数等于或高于所选值，则邮件将归类为垃圾邮件。 可移动滑动块对分数进行更改。
拒绝邮件所需的分数	若邮件分数等于或高于所选值，则邮件将被拒绝。 可移动滑动块对分数进行更改。

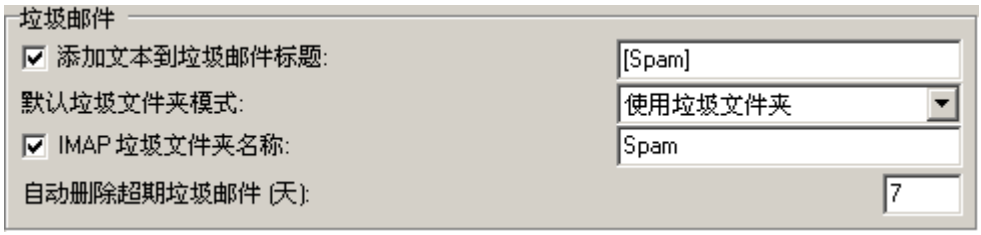
注意：隔离的邮件被暂存在一个待决队列中，直到被授权、或手工投递或被拒绝。

验证可以通过手动方式（用户或域管理员使用 WebAdmin 或 WebClient），也可以是自动的（发送方对验证回复邮件作出响应）（参见 **反垃圾 -- 隔离**）。

删除可以是手动的（用户或域管理员使用 WebAdmin 或 WebMail），也可以是自动的（在爱思华宝内进行设置）（参见 **反垃圾 -- 隔离** ）。

手动投递则只能由用户或域管理员通过 WebClinet 或 WebAdmin 进行。

字段	描述
拒绝邮件动作	针对被拒绝的邮件选择一个动作。 **删除** 选择此选项，爱思华宝服务器将在不通知发送方服务器的情况下"删除"邮件，因此发送方将不能获得任何返回信息。 **拒绝** 选择此选项，爱思华宝服务器将拒绝接收邮件，并向发送方服务器返回一条通知信息。
归档拒绝邮件到帐户	选择一个帐户，以便将被拒绝邮件归档至帐户中。 使用 按钮打开 **帐户选择** 对话框。 不管是否选择上述删除或拒绝选项，此选项均有效。



字段	描述
添加文本到垃圾邮件标题	此选项用于将文字添加至被认为是垃圾邮件的信息的主题。 在文本框内设定所要添加的文本。 应注意，此字段可使用系统变量，如上一屏幕截图所示。 例如： 若一条邮件被识别为垃圾邮件，则其原有主题 ***Cheap Meds Here*** 您的此处文本框设定为 ***[Spam %%SpamScore%%]*** 如果被判定为垃圾邮件，那么标题将改变为类似以下内容 ***[Spam 5.97] Cheap Meds Here*** 这就使用户可以对邮件客户端规则进行设定，以处理可疑垃圾邮件。

默认垃圾邮件文件夹模式	选择用户是否启用垃圾邮件文件夹。 ▪ ***使用垃圾邮件文件夹*** 邮件被标记为垃圾邮件后，不保存到用户的收件箱，而保存到一个单独的垃圾邮件文件夹。你可以进一步定义垃圾邮件管理员以便维护一个或多个垃圾邮件文件夹。 这能大大节省一个忙碌的主管人员的时间，允许一个助手帮助主管检查他们的垃圾邮件文件夹并将正常的邮件从垃圾邮件夹中移至收件箱。 ▪ ***不使用垃圾邮件文件夹*** 所有邮件 - 包括垃圾邮件和正常邮件都被保存在收件箱文件夹。 注意 是否使用垃圾邮件文件夹取决于他是否使用 IMAP (包括在 WebClient) 。 有两种方式禁用个别用户使用垃圾邮件文件夹： 1) 用户设置 - 选项 - 垃圾邮件文件夹模式 = 禁用 2) 用户设置 - 选项 - 垃圾邮件文件夹模式 = 默认，反垃圾 - 动作 - 设置垃圾邮件到垃圾邮件文件夹 = 禁用
IMAP 垃圾文件夹名称	此选项用于将垃圾邮件文件夹与 IMAP 帐户进行集成。 输入用于垃圾邮件的 IMAP 文件夹名称。
自动删除超期垃圾邮件（天）	垃圾邮件文件夹内的邮件在所设定的天数之后，将被自动删除。

报告

字段	**描述**
启用隔离报告	此选项用于将隔离邮件报告发送至所有被隔离邮件的收件人用户。
启用垃圾文件夹报告	发送垃圾邮件报告给用户。
计划任务	用于设定隔离报告的发送方式及发送时间。一个标准的计划任务对话框将打开。

立即运行	立即运行垃圾邮件报告。
发件人	隔离报告邮件的发件人选项中出现的名字。此处应该填入一些有意义的说明。
发自	隔离报告邮件中邮件头 from 出现的值，将会在用户回复该邮件时做为收件人出现。
报告模式	选择以下操作之一： **新条目**- 隔离报告中仅显示上次报告后新添加的条目。 **所有条目** - 隔离报告包中含了所有隔离条目。
日志级别	选择一个反垃圾日志的级别： ▪ **无**–没有任何日志. ▪ **摘要**–只有垃圾邮件被记录. ▪ **调试**–所有邮件和动作都被记录 ▪ **扩展**–对于本服务来说，和 调试 相同
URL	输入爱思华宝服务器确认页面的 URL。 定义该功能使用的端口(端口 80)。 如果是多域名服务器，需要使用系统变量%%Recipient_Domain%% 例如：variable %%Recipient_Domain%% like so **http://%%Recipient_Domain%%:32000/reports/** 以上的设置是使用接收者的域后缀，所以如果一封邮件是发给 john@icewarpdemo.com 会使用 **http://icewarpdemo.com:32000/reports** 注意：该功能的运行是在爱思华宝服务器 Web 服务正常运行的前提下。

注意：反垃圾报告是通过 Web 服务启动。

此处有三个变量与垃圾邮件报告有关：

- ***SpamLang*** **–**设定垃圾邮件报告的语言
- ***SpamReportsDateFormat*** **–**设定垃圾邮件报告将使用的日期格式
- ***SpamReportsTimeFormat*** **–**设定垃圾邮件报告将使用的时间格式

它们能通过 API 控制台进行修改。

相应格式说明位于 ***http://cz2.php.net/manual/en/function.date.php***.

如何设置反垃圾报告

1. 启用报告

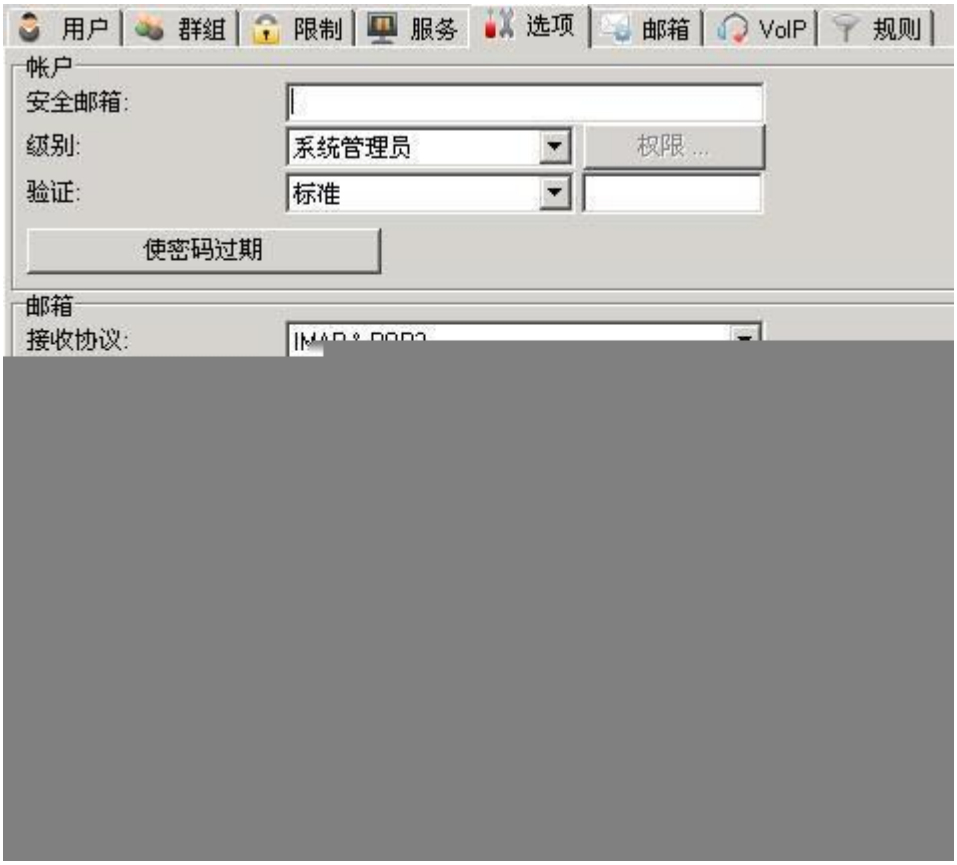
   导航到 反垃圾 - 动作节点 - 动作选项卡 - 反垃圾部份 并设置 默认垃圾文件夹模式 字段为 使用垃圾文件夹 。

导航到 **反垃圾 - 动作节点 - 报告** 选项卡，启用报告 (勾选单选框)，设置 *计划任务*、*发件人*、*发自*、*报告模式* 和 *URL*。

2. 指定将使用报告的用户

现在，报告已在服务器上的所有用户中启用，如果您想仅为指定用户或域使用报告，您需要在用户级修改设置。

导航到 **管理 -<域> -<用户> - 选项卡 - 反垃圾** 部份并设置 反垃圾报告模式 以及 **垃圾文件夹模式**。（更多相关信息，请参考 F1 帮助中的相关说明）。



3. 使用 tool.exe

虽然您可以使用 GUI 来改变设置，但手工修改所有域/用户的设置仍然不太方便。

因此您可以使用 tool 来做这些修改，启动内置的文件管理器(在 GUI 工具栏中点击相应图标或按下 CTRL+SHIFT+F)，然后使用命令行运行命令。

tool set account *@* U_QuarantineReports x

****@* – all accounts on the server***

****@domain.com – all accounts at "domain.com"***

user@domain.com – "user@domain.com" only

其中 x 的意思是：

0 - 禁用

1 - 默认

2 - 仅新条目

3 - 所有条目

示例:

您想使用报告但不想包括某些域。

如果您执行步骤 #1，则所有用户将收到邮件，您可能想排除一些域：

tool set account *@<domain> U_QuarantineReports 0

替换 <***domain***> 为相应的域名。

另一选择是在 spam/reports/ 文件夹下建立 bypass.dat 文件，该文件包含一个在报告处理时将被忽略的域列表。 这对于备份域是非常重要，因为它没有用户，因些推荐对备份域进行忽略处理，请为每个域独占一行。

您仅想为一个域使用报告。

最简单地实现方法是首先禁用所有的报告，然后再启用您指定的域。

tool set account *@* U_QuarantineReports 0

这将禁用所有用户的报告（根据服务器上用户数量的不同，处理可能需要一些时间）。

然后再为指定域/用户启用报告：

tool set account *@<domain> U_QuarantineReports 1

注意：默认的意思是 反垃圾 - 动作节点 - 报告选项卡 的选项。

您想为不同的域使用不同的设置。

您可能想为一些域使用 所有项目 并为其他域使用 新项目。步骤取决于使用哪个设置的域更多，假如 80% 的域使用 所有项目， 则最简单的方法是设置默认模式为 所有项目(参考步骤 #1)， 然后再改变指定域的模式。

tool set account *@<domain> U_QuarantineReports 2

注意：对于备份域，只有隔离报告才发送，如果您想每一个垃圾邮件都发送报告，设置垃圾邮件计分 (反垃圾 - 动作 - 动作选项卡 - 标记为垃圾邮件所需的分数) 等于或高于 隔离一封邮件所需的分数 (位于同一选项卡)。

只有备份域内帐户的用户可以访问他们的隔离队列而无需等待隔离报告。他们可以如下操作：

* 在浏览器地址栏中输入以下地址：

<icewarp_server_hostname>/admin/index.html?view=gateway_login***<icewarp_server_hostname>/admin/index.html?view=gateway_login***

* 输入 电子邮件地址 和 验证码 字段。

* 然后该链接将显示他们当前的隔离区，该连接将通过邮件地址发送到相应邮箱。

不同的报告时间表

你可能想为一些用户或域设置不同的报告时间表，可实现它，按以下步骤操作：

1. 创建 bypass.dat 文件并将其插入到 <InstallDirectory>/spam/reports 文件夹。
2. 进入文件，插入你想例外的用户和/或域 -- 每行一个。

   对于用户的结构是： <user's_email_address>

   对于域的结构时：***<domain>***

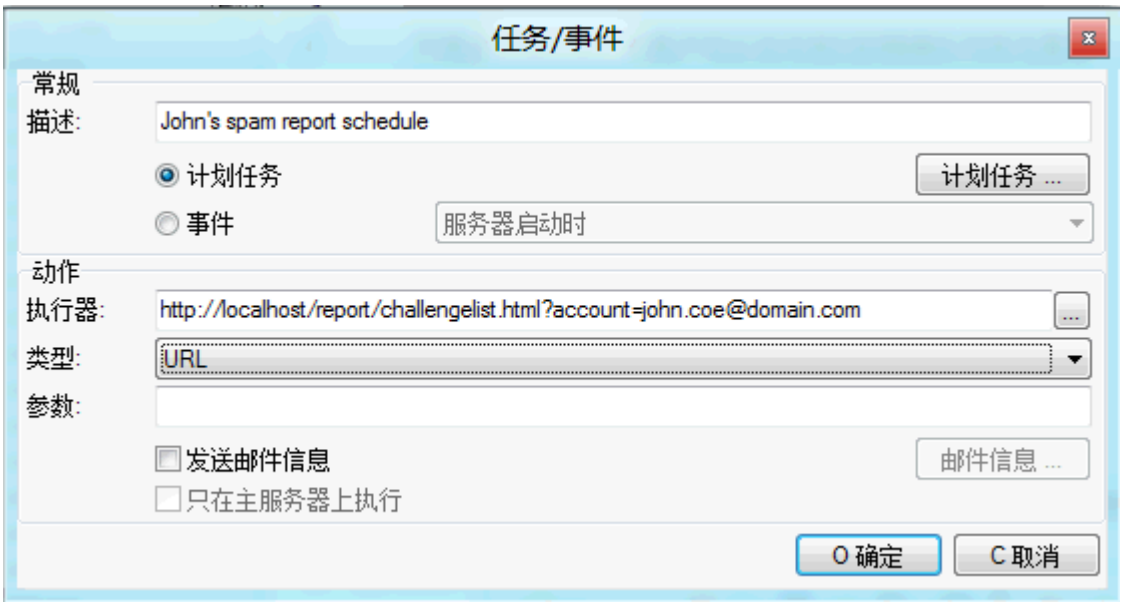
   例如：

   john.doe@domain.com

   alison.w@domain.com

   domain2.com

   在通用的垃圾报告时间表中将排除这个用户。
3. 创建一个新的任务 （系统 -- 工具 -- 计划任务）。



点击 ***计划任务*** 按钮并设置希望的个人时间表。

在 ***类型*** 字段，选择 URL 选项，输入相应的 URL 到 ***执行器*** 字段。

结构是：

对于用户：***http://localhost/reports/challengelist.html?account=<user's_email_address>***

例如：***http://localhost/reports/challengelist.html?account=john.doe@domain.com***

对于域：***http://localhost/reports/challengelist.html?domain=<domain>***

例如：***http://localhost/reports/challengelist.html?domain=domain2.com***

不要忘记勾选 ***只在主服务器上执行*** 选项。

注意：要获得使用该执行器报告的详细信息，请使用 API 控制台设置以下变量为相应的值：SpamReportsDebugLevel=1, SpamReportsLogLevel=4.

请注意： 报告 URL 可以被任何人执行，即使是远程用户（只要你用户的邮件地址可见）。为阻止这种情况，你可以设置 **SpamReports*** 的值为 0 (故障将立即解除) 或保护 report 只能在你服务器上运行。

URI = /reports/challengelist.html

IP = NOT 127.0.0.1

ACCESS = DENY

另请注意： 调试日志可能浪费造成对资源的浪费。

注意：要获得使用该程序的详细报告，使用 API 控制台设置以下变量为相应的值： SpamReportsDebugLevel=1, SpamReportsLogLevel=4

隔离

爱思华宝服务器的隔离功能允许你将接收到的邮件排列在待决队列中，并等待被许可。

用户可通过 WebClient 对各自的待解决队列进行管理。

域管理员可通过 WebClient 或 WebAdmin 对所有待解决邮件进行管理。

对于待解决邮件，有以下选项：

- **授权**-发送邮件并将发送方添加至隔离白名单中，此发送方以后发出的邮件都不会被隔离。
- **投递**- 发送邮件至收件人，但并不将发送方添加至白名单中。
- **黑名单**-仅简单地从待解决队列中将邮件删除。

您可以设定用户发送邮件的外部收件人自动添加至白名单中(参见 ***动作***)

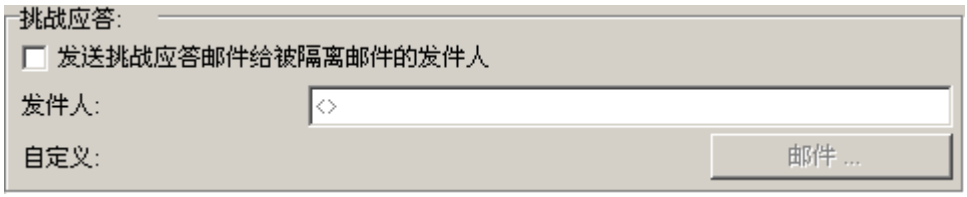
你也可以激活 ***挑战-应答*** 系统功能，由此未经授权的发送方可通过访问网站证明他是一个实实在在的发送人（参见本部分下文）

在管理主控台或 WebAdmin 中的 垃圾邮件队列 节点中，可以看到待决队列的状态和隔离白名单。

字段	描述
激活	激活隔离功能。
隔离	按下按钮，跳至垃圾邮件队列中的垃圾邮件队列 节点。

注意： 该服务的访问模式可从域和用户级别设置，请参见相应位置（**[域] -- 策略， [用户] --策略**）。

字段	描述
移除待定邮件期限	指定隔离区中邮件的保存天数。
到期邮件标为垃圾投递至用户邮箱	隔离区中的邮件到期后将被标为垃圾邮件投递到用户的垃圾邮件夹。



挑战应答是通过爱思华宝服务器投递一封包含一个 URL 的邮件给发件人，且发件人必须经过一个确认的过程（参见 **如何工作** 部份）。

这使用 Web 管理员和 WeClient 一样的引擎。

字段	**描述**
发送挑战响应邮件给被隔离邮件的发件人	选择该选项将有一个挑战响应邮件发送给被隔离邮件的发件人。 注意，为确保该功能正常工作，你必须在 ***系统-服务- 自动发现*** ？URL 部分正确设置反垃圾报告的 URL。
发件人	在此处指定 SMTP 协议中将会使用的发送方。 我们建议使用默认（**空白**）选项，并不推荐对其做出更改，因为这将减少不受欢迎的自动响应。
自定义	按下 邮件 按钮，对挑战应答的邮件内容进行自定义设置。 邮件对话框将打开，并允许你对 来自：与主题：的标题选项以及信息正文内容进行设置。 你可以使用信息正文中的系统变量进行设置。 应注意的是，特殊变量 %s 必须包含在信息正文中，因为这个变量包含需要访问的 URL。

例子:

下面的确认请求邮件由邮箱管理系统生成，此信息是为了对向用户 ***xxx@webmail.domaina.com*** 发送信息的发送方 ***user@icewarpdemo.com*** 做出响应。

反垃圾邮件报告 URL:**http://%%Recipient_Domain%%:32000/challenge/**

来自：

至： <user@icewarpdemo.com>

接收自： webmail.domaina.com

由 SMTP id 为 DEMO 的 mail.icewarpdemo.com（icewarp mail server 9.0.0.5）接收

收件人为 *user@icewarpdemo.com*; 2004 年 3 月 7 日，星期日，01:48:16 +0100

日期： 2004 年 3 月 7 日，星期日，01:48:16 +0100

来自： 询问响应<info@icewarpdemo.com>

至： xxx@webmail.domaina.com

信息 Id： <812060168@mail.icewarpdemo.com>

主题： [询问响应]访问此 URL 以确认邮件

http://mail.icewarpdemo.com:32000/challenge/?folder=c42c1a770e2d6d07ff358b2c22d7cf71

为了证明接收到的信息是由实实在在的发送人发送而不是由计算机发送，需访问下面的 URL，并键入图像中能看到的混合符号文本。对于此邮件地址，仅需一次验证操作。

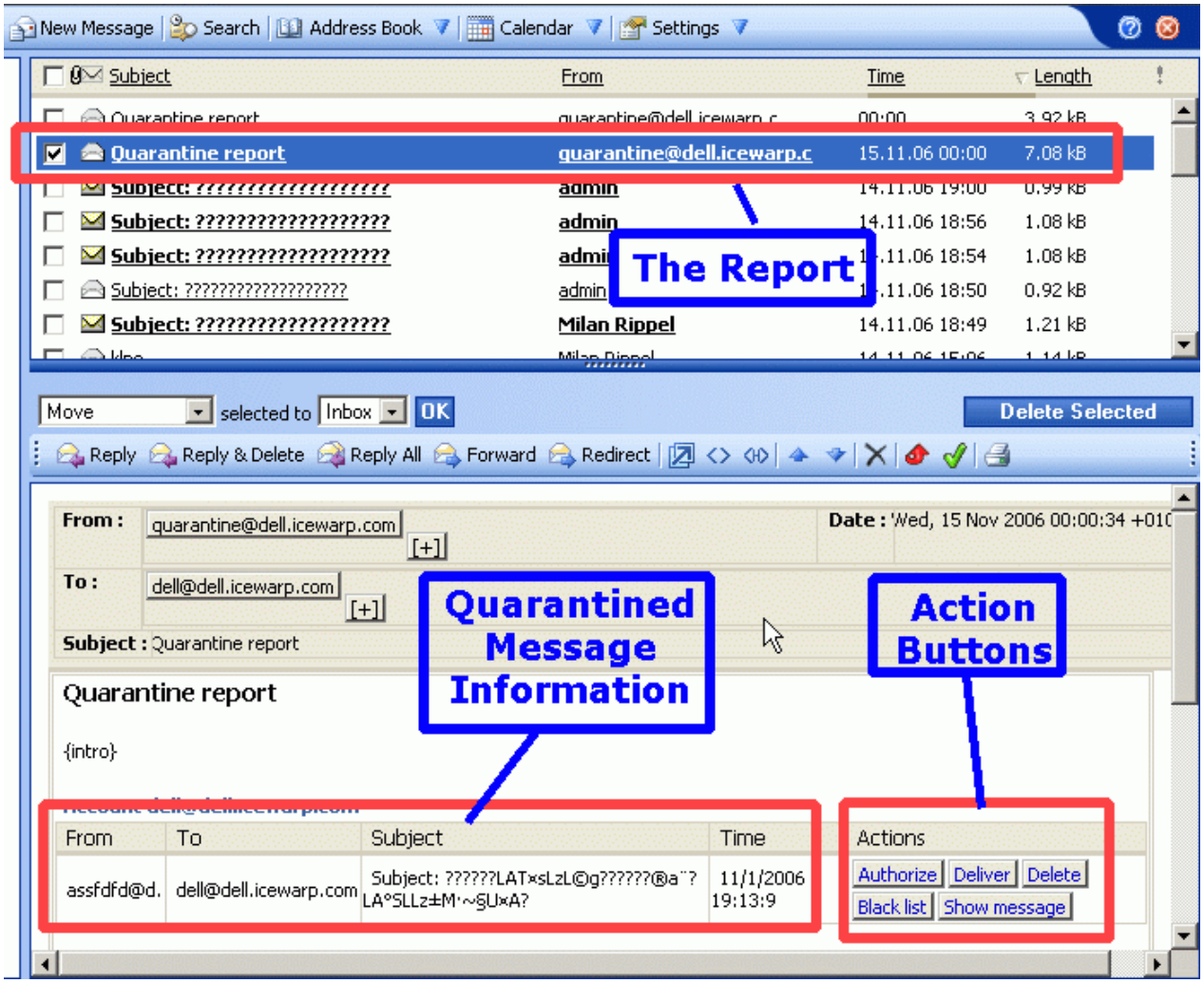
http://webmail.domaina.com:32000/challenge/?folder=c42c1a770e2d6d07ff358b2c22d7cf71

本章内容

隔离 - 隔离报告 20
隔离 处理接收的邮件.....22
隔离 - 处理队列中的邮件.....23
挑战响应 - 如何工作 24

隔离 - 隔离报告

若激活此功能，则每个隔离用户都将收到一个列出隔离邮件的邮件报告，这些邮件带有可点击的链接以将邮件激活：



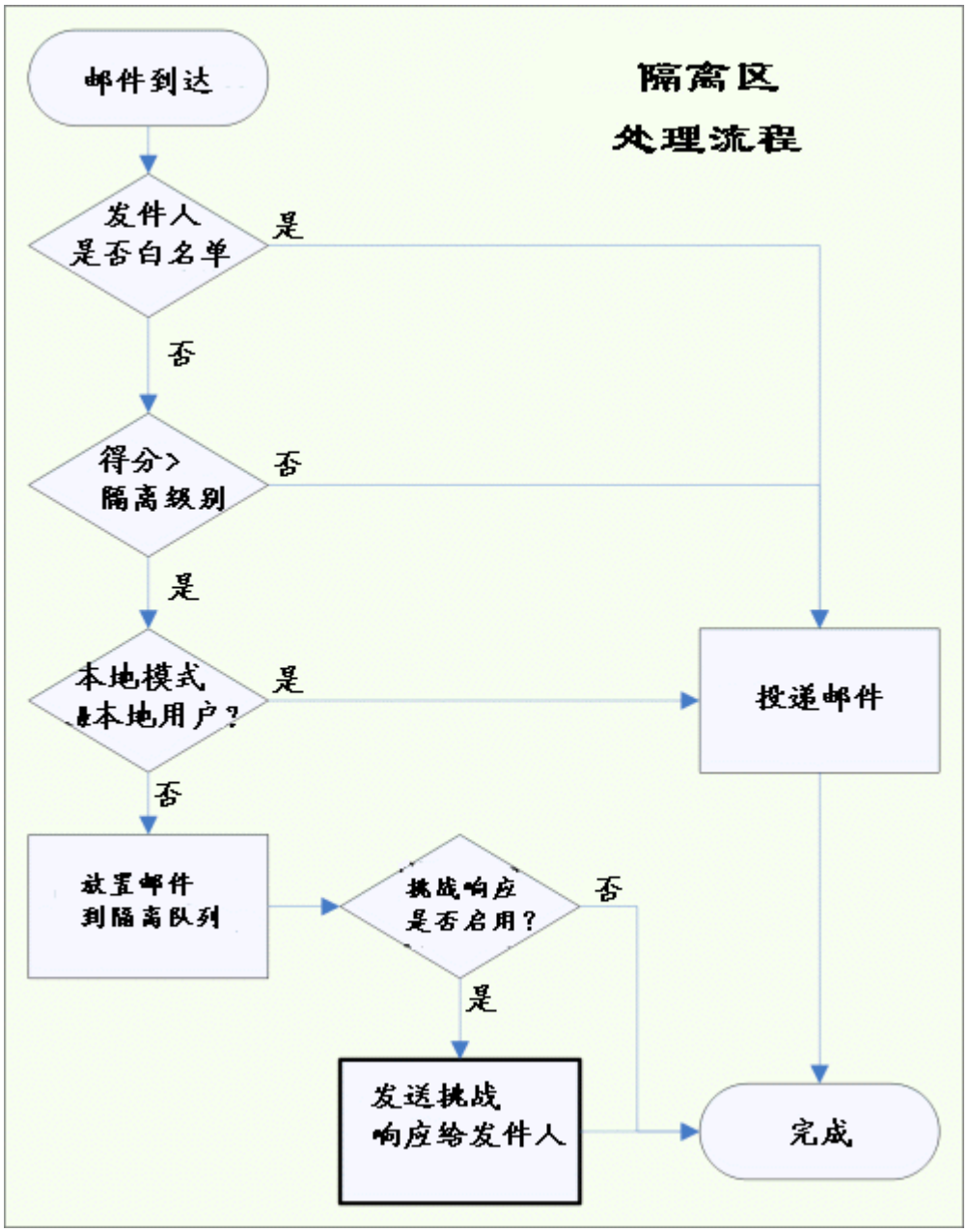
上面截图显示了信息的详细内容，动作按钮设置对于处理信息是非常有用的。

按钮	动作
授权	投递邮件并白名单发件人。
投递	投递邮件到收件人。
删除	删除邮件。
黑名单	增加发件人到黑名单。
显示邮件	打开一个新的浏览器窗口窗口窗以文本格式显示邮件(包含信头在内)。

隔离 处理接收的邮件

如果启用 隔离 功能，将根据隔离白名单对所有入站邮件的发送者进行核查。如果发送者包含在白名单内，则按正常方式处理邮件。如果发送者不在白名单中，则信息需在隔离待处理队列中等候处理。

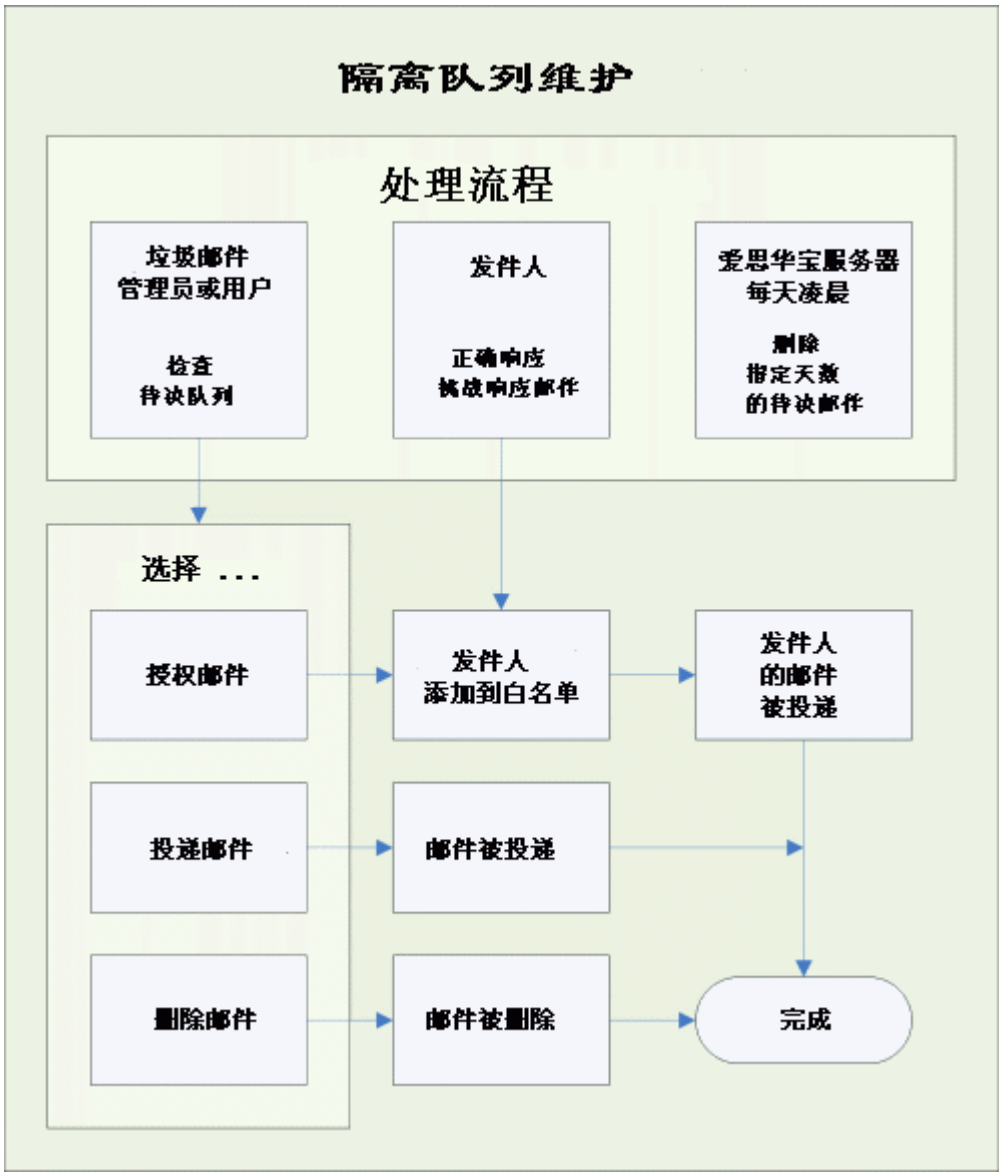
此外，如果激活挑战响应系统，则将发送询问响应邮件至发送者，这就使发送者可以通过访问网页来证实自己是实实在在的发送人。



隔离 - 处理队列中的邮件

可通过多种方法对位于待决队列中的邮件进行处理：

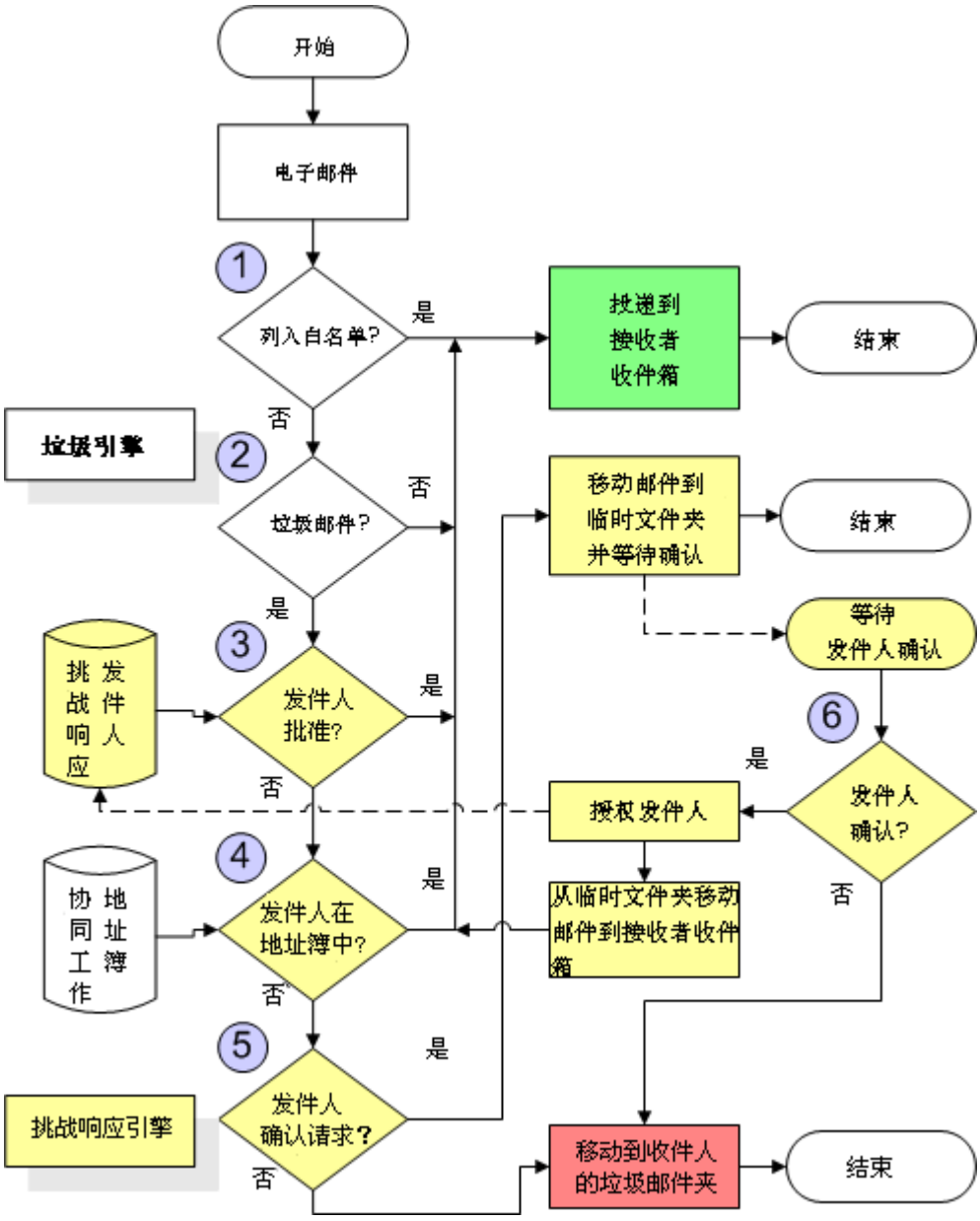
- 发送者对询问响应邮件作出正确回应，并自己授权。
- 用户通过 WebClient 界面核查隔离队列，并选择授权、发送或删除一条或多条信息。
- 垃圾邮件管理员通过网邮界面或管理员主控台对所负责的任何隔离队列进行核查，并选择授权、发送或删除一条或多条信息。
- 在设定的天数之后，爱思华宝服务器自动将邮件删除。
- 下图为处理过程的流程图：



挑战响应 - 如何工作

挑战响应系统要求邮件发送者证实他/她的确发送了邮件。发送者必须通过访问网页并输入代码进行确认。

挑战响应系统是完整的反垃圾邮件解决方案的重要组成部分。下图中的 黄色组件 即为完整的即时反垃圾邮件数据图表。



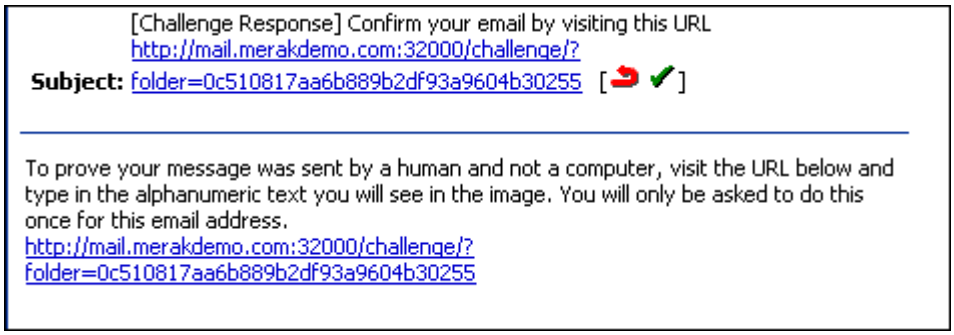
在一般的典型情况下，邮件是在通过所有黑白名单（如黑名单与白名单技术中所述）判定之后才到达挑战/应答系统，且已被标记为垃圾邮件。

- 服务器在收到邮件后，并不发送至收件人，而是存储在临时文件夹中。如果相同发送者发送多条信息，则所有信息都将存储在相同的文件夹中。这些信息被标记为待处理邮件，如果待处理信息在设定的天数内未被授权，则将自动被删除。
- 服务器将生成确认请求，并发送至邮件发送者。它使用的是 SMTP 协议中的发送者，与邮件中显示的 Mail From：可能不同。
- 发送者（如果存在）将收到确认请求，且必须对其进行确认。此确认请求需要访问一个特殊的网页，并在一个文本字段内输入相应字符。输入字符以避免自动确认系统的使用。
- 服务器将接收到来自发送者的确认邮件并将之前的邮件发送至收件人。此发送者也将添加至 “允许发送者名单”，下次发送邮件时将无须再次确认。

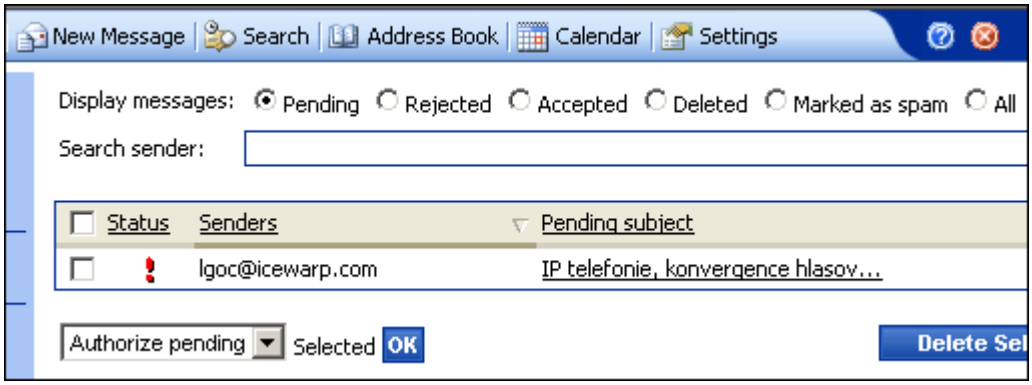
邮件来自于字段空白的邮件（在 SMTP 会话中类似于来自于：<>）会绕开挑战响应引擎。对于类似的邮件，应使用内容过滤器或黑&白名单。

屏幕截图举例：

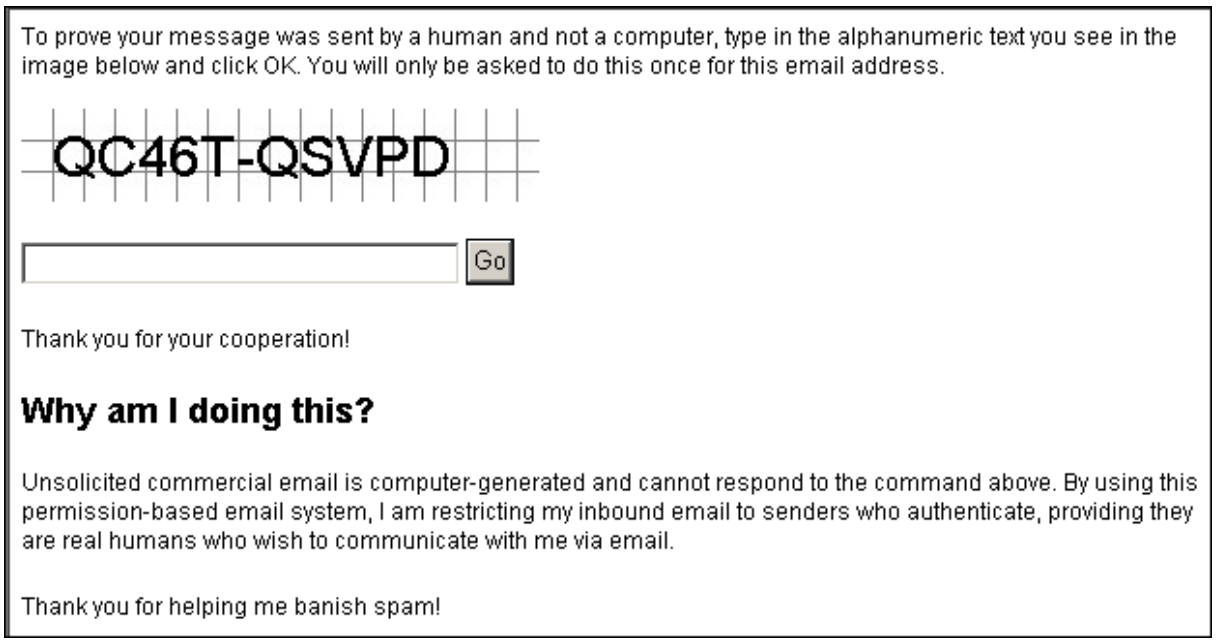
邮箱管理系统发给发送者的确认请求



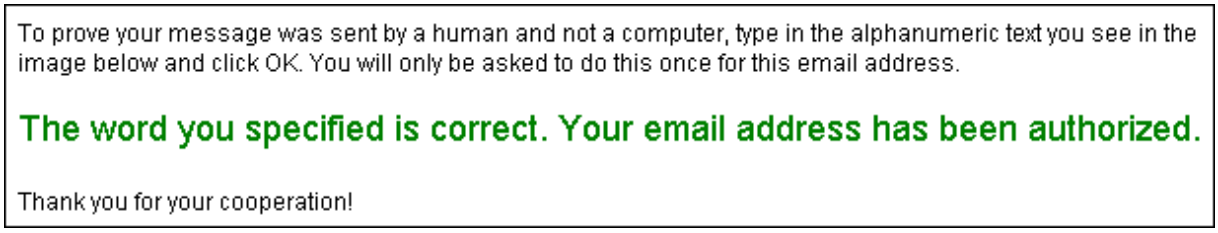
待授权的发送者 在数据库中等待解决



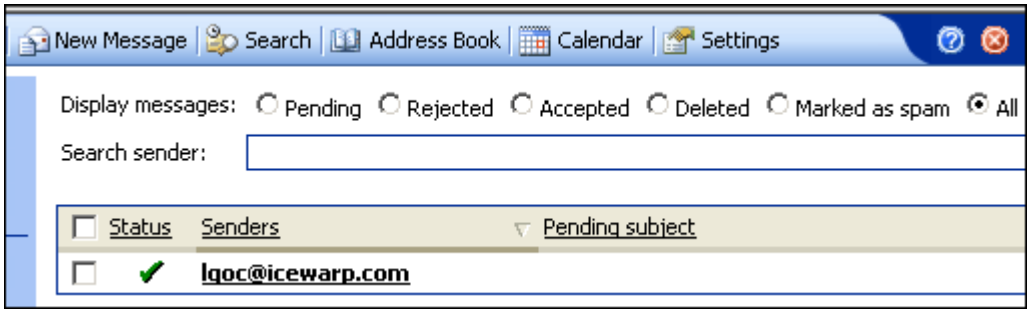
发送者确认请求的网页 URL



发送者如输入正确代码，则自动被授权。



被授权的发送者将被添加至询问响应中。



根据询问响应系统设置的不同，被授权的发送者可针对服务器上的一个收件人或所有收件人。

反垃圾 - 垃圾杀手

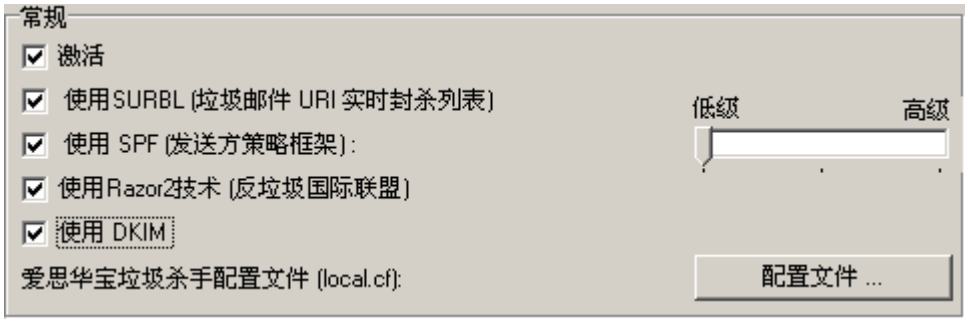
SpamAssassin 是一个致力于反垃圾邮件的开源项目。所提供的软件通过一套复杂的规则检查一封邮件是垃圾邮件还是合法邮件。这些规则主要针对典型的垃圾邮件模板进行检查。

在新的反垃圾邮件技术引入的同时，这些规则也不断地被更新。

垃圾杀手在识别专门欺骗用户以泄露财产信息的 钓鱼邮件上有很大的优势。

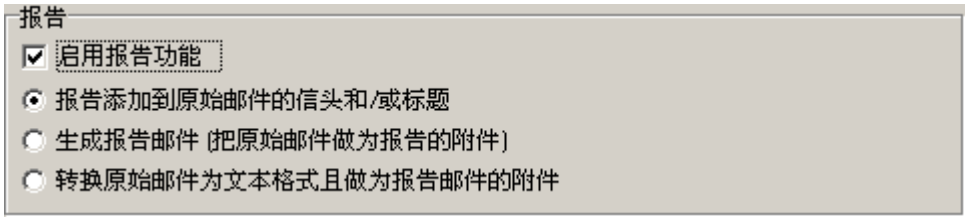
它通过一系列广泛的本地和网络检查对垃圾邮件特征进行识别。这就使垃圾邮件制造者更难找出散布其信息的方法，

爱思华宝采用垃圾邮件杀手规则，但使用内部自有引擎进行处理。



字段	描述
激活	使用垃圾杀手过滤器。 此为推荐选项。
使用 SURBL	此选项用于使用垃圾邮件 URL 实时拦截列表技术。 SURBL 并非对垃圾邮件发送者进行识别，而是对邮件正文的 URL 中出现的垃圾邮件主机进行识别。对于垃圾邮件制造者来说，更改主机 URL 比更改任何其他信息都要难的多，因此，这是识别垃圾邮件的一个可靠方法。 SURBL 是识别 Phishing 来源的一个很好的方法，即以发送信息并试图通过银行登录或信用卡详细信息来欺骗用户而著称的来源。 可登录 http://www.surbl.org 网站了解更多信息。
使用 SPF	此选项用于使用 SPF（发送方策略框架）技术。 SPF 技术通过使用 DNS 决定所报告的来自一个域名或源自某个域名的信息是否合法。它所依靠的是公布的 DNS 记录，但也不全是这样，softfail 可能会发生，而在技术认为发送主机为非法时却不能确定。 使用滑动块设定当 SPF 检查返回 softfail，爱思华宝将采取什么措施。 低 添加 0.1 至垃圾邮件分数 中 添加 0.5 至垃圾邮件分数 高 添加 5.0 至垃圾邮件分数 此项非常严格！ 请访问 http://www.openspf.org/ 网站了解 SPF 介绍信息。

使用 Razor2	选择此选项，则爱思华宝服务器可使用 Razor2 反垃圾邮件技术。 SURBL 并非对垃圾邮件发送者进行识别，而是对邮件正文的 URL 中出现的垃圾邮件主机进行识别。对于垃圾邮件制造者来说，更改主机 URL 比更改任何其他信息都要难的多，因此，这是识别垃圾邮件的一个可靠方法。 SURBL 是识别 Phishing 来源的一个很好的方法，即以发送信息并试图通过银行登录或信用卡详细信息来欺骗用户而著称的来源。 可登录 http://www.surbl.org 网站了解更多信息。 注意 - 为使 Razor2 正常运行，需打开防火墙与/或路由器上的端口 2703。
使用 DKIM	此选项用于激活域密钥技术。 登录 http://antispam.yahoo.com/domainkeys 网站可查看完整的介绍信息。 如果来自具有 DNS 域密钥记录的进入电子邮件未被签名，则垃圾邮件总分会增加。 如果进入的电子邮件完全未被签名，则分数也会增加（但增加的数量低于第一种情况）。
配置文件	按下按钮，打开垃圾杀手配置文件。 请不要更改此文件中的任何选项，除非确定有更改的必要和把握。



字段	描述
启用报告功能	选择此选项，激活垃圾杀手的报告功能。 选择三个选项中的一个，设定报告的方式。
报告添加到原始邮件的信头和/或主题	报告将被添加到接收到邮件的信头. 注意 - 此为推荐选项。
生成报告邮件(把原始信息附加到报告)	垃圾杀手报告邮件将被接收，原始邮件将做为附件。
转换原始邮件为文本格式且做为报告邮件的附件	接收到的垃圾杀手报告邮件，并将原始信息作为文本文件附在文后。

输入一个 ***目录/文件名***，过滤统计记录到一个文件。你可以使用文件名采用 ***YYYYMMDD*** 风格。

RBL

字段	描述
激活	使用 RBL 服务器。
RBL 服务器列表	选择你想要使用的 RBL 服务器。 注意 - 要限制 RBL 服务器选择的数量，选择太多会影响服务器性能，因为每封邮件都要到 RBL 服务器上进行查询，增加处理的开销。 如果 DNSBL 主机数超过 4 个，一个警告提示将出现。 一个 RBL 中包含有 IP 地址列表，这些 IP 地址的使用者拒绝停止将垃圾邮件从服务器中传播出去。RBL 通常列出网络服务提供商，它们的客户对那些垃圾邮件或被垃圾邮件制造者用来发送垃圾邮件的服务器负责。 注意 同时支持扩展的 RBL 节点，可登录 http://www.us.sorbs.net/using.shtml 了解进一步的信息。 若使用 *dnsbl.sorbs.net* 作为 RBL，则会返回一个代码，表明哪一个或多个黑名单中包含有一个项。 举例： 对于一个开放的 SOCKS 服务器，返回 127.0.0.3 对于一个开放的 SMTP 中继服务器，返回 127.0.0.5 注意：列表中有两个 *dnsbl.sorbs.net* 条目（标为 (A) 和 （B））。这是两个不同的规则，如果您决定使用他，请选择其中一个。

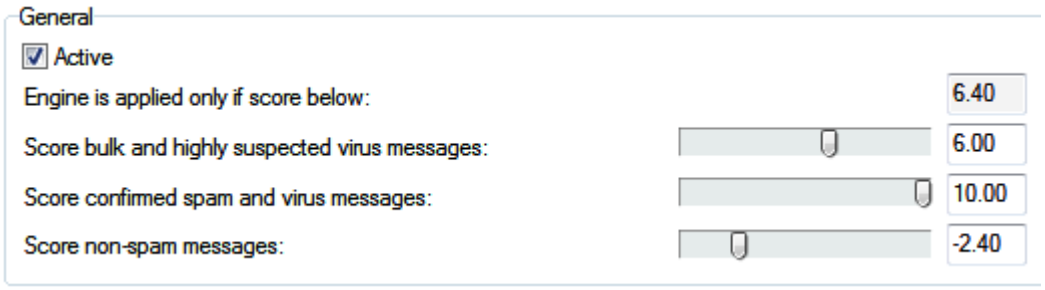
爱思华宝在线反垃圾

爱思华宝服务器能够使用在线反垃圾(一个基于 RPD(重复样本检测)技术的应用)，做为对抗垃圾邮件的一部份。

实时检测中心分析互联网上巨量的实时流量，从广泛分布的样本特征码中识别出新垃圾邮件、病毒和钓鱼攻击的爆发。新爆发的攻击通常在发生后的片刻时间内就被立即更新到联网服务器上。

这能有效的保护你的用户，避免其受到广告和垃圾邮件的骚扰。

与其它集成在爱思华宝服务器内部的反垃圾技术一样，在线反垃圾通过调整一封邮件的垃圾得分，从而决定对邮件的最终判断：



字段	描述
激活	启用 CommTouch 检测。 **(Commtouch** 技术能够自动分析全球网上数以亿计实时邮件数据，以确定新的威胁，保护电子邮件安全)
应用引擎,当得分低于:	该字段显示一个限制爱思华宝在线反垃圾引擎运行的分数。 一封邮件进入到爱思华宝在线反垃圾时均带有一些垃圾得分。在 正常邮件计分 ，你能设置一个爱思华宝在线反垃圾引擎认为正常邮件的计分（一般为负数），该分数将被添加到被在线反垃圾处理前的得分中。如果该分数高于 在 ***反垃圾 - 动作*** - 标记为垃圾邮件的分数字段所设置的值，则它因为毫无意义而不被爱思华宝在线服务器处理，因为该邮件仍是垃圾邮件。 例如： 您设置 *标为垃圾邮件* ... 值设置为 4。 在线反垃圾的 *正常邮件计分* 为 -2.6 邮件进入爱思华宝在线反垃圾处理前的 得分为 7。 7 - 2.4 = 4.6 该邮件因为得分高于 4 - 它将不被爱思华宝在线反垃圾处理。 其他示例： 邮件进入爱思华宝在线反垃圾处理前的得分是 5。 5 - 2.4 = 2.6 爱思华宝在线反垃圾将运行。

群发及疑似病毒邮件计分	设置该滑块到指定数值，当在线反垃圾报告邮件为群发邮件时该数值将被添加到邮件的垃圾得分。
已确定的垃圾和病毒邮件计分	设置该滑块到指定数值，当在线反垃圾报告邮件为垃圾邮件时该数值将被添加到邮件的垃圾得分。 基于在线反垃圾的高可靠性，推荐该值在 9 分或以上。
正常邮件计分	设置该滑块到指定数值，在线反垃圾判断为正常邮件时，将减少该数值到垃圾邮件得分。

注意 - 在线反垃圾引擎仅检查没有被爱思华宝服务器的其它反垃圾引擎归类为垃圾的邮件，根据 ***反垃圾动作 - 常规*** 中的 ***判断为一封垃圾邮件所需的分数*** 中的设置。

动作 - 常规 爱思华宝在线反垃圾原因 **- 在线识别=**

代码	**原因**
Y	邮件被在线反垃圾服务器标记为高疑似垃圾邮件。
H	该邮件被标记为高疑似广告邮件。
N	该邮件被确认为正常邮件。

注意：一些服务器阻止外部 80 端口的访问，因此防火墙需要知道在线反垃圾的具体地址，该信息可以在 **ctasd.conf** 文件看到 **(<InstallDirectory>/spam/commtouch)**:

Server_address = Resolver%d.icew.ctmail.com

其中 ***%d*** 是一些动态数字。

本章内容

爱思华宝在线反垃圾 分级.....31

爱思华宝在线反垃圾 分级

该表格显示一个分类参考，关于爱思华宝在线反垃圾返回给爱思华宝服务器的各种原因码的具体解释。

这些爱思华宝在线反垃圾级别能在反垃圾日志之内定位。

反垃圾日志示例:

209.85.28.205 [1108] 05:19:44 PSC07843 '<cli10176@someone.com>' '<me@icewarpdemo.com>' 1 score 10.00 reason [SpamAssassin=1.60,Body=PE,**Live=H**,Sender] action SPAM

和/或 邮件 X_CTCH 信头内

X-CTCH 信头行实例

X-CTCH: RefID="str=0001.0A090206.48EDBE9F.0245,ss=3,fgs=0"; *Spam="Bulk"*; *VOD="Unknown"*

注意，如果邮件 ***不包含*** 一个 X-CTCH 信头，则它 不能 通过爱思华宝在线反垃圾服务分类并不会得到报告!

X-CTCH 信头	**解释**	**爱思华宝服务器原因码**	**条件 mis-classified 是...**	**报告邮件至用户...**
Spam=Confirmed	邮件来自于一个已知的垃圾邮件源。	LIVE=Y	误报	aslive-genuine
Spam=Bulk	邮件不是从一个已知的垃圾邮件源发出，但是具有群发邮件的特征。	LIVE=H	误报	aslive-genuine
Spam=Suspect 查看下列的注意事项 1	邮件不是来自一个已知的垃圾邮件源，但是比高于正常发送。	LIVE=N	漏报	aslive-spam
Spam=Unknown	邮件不是来自已知的垃圾邮件源并且是一个正常派发。	LIVE=N	漏报	aslive-spam
Spam=Non-spam	邮件来自爱思华宝在线反垃圾信任源。	LIVE=N	漏报	aslive-spam
VOD=Virus	邮件包含恶意软件	LIVE=Y	误报	aslive-genuine
VOD=High	邮件高度可疑是包含恶意软件	LIVE=H	误报	aslive-genuine
VOD=Medium 查看下列注意事项 2	邮件怀疑包含恶意软件	LIVE=N	查看下列注意事项 2	查看下列注意事项 2
VOD=Unknown 查看下列注意事项 2	不确定的威胁级别	LIVE=N	查看下列注意事项 2	查看下列注意事项 2

VOD=Non-virus 查看下列注意事项 2	邮件确认作为恶意软件=免费	LIVE=N	查看下列注意事项 2	S 查看下列注意事项 2

注意 1 - Spam=Suspect 现在不再支持并不会发生。如果仍有，爱思华宝服务器将归类为合法邮件。

注意 2 - 爱思华宝在线反垃圾不会替代爱思华宝服务器 AV 引擎，对于病毒，爱思华宝在线反垃圾仅会在一个新病毒首次爆发时的几分钟内使用，同样地爱思华宝服务器只会在邮件包含病毒的最高概率时做出反应。因此不能与 AS 病毒检测相比。

报告错误的分类

如果邮件是一封正常邮件请报告误报到 **aslive-genuine@icewarp.cn** ，产品确认书，newsletter 等容易标为垃圾邮件/病毒。该邮箱仅接受合法具有分级的分类:**Spam ="Confirmed "/"Bulk"**和 **VOD="Virus"/"High"**。不要发送其他分级的邮件！

如果邮件是一个垃圾邮件报告误报至 **aslive-spam@icewarp.cn** ，网络钓鱼，诈骗或欺骗没有标记。该邮箱接受以下分级的垃圾邮件: **spam="Suspect"/"Unknown"/"Non-spam"**。不报告病毒，恶意软件或具有其他分级的垃圾邮件！

语言码使用与邮件语言相对应的。例如，如果该邮件是捷克语，你应该转发邮件至 aslive-genuine@icewarp.cz 或 aslive-spam@icewarp.cz 。

如果没有相应的国家代码，邮件应该发送给 **support@icewarp.com** ，我们的支持团队将尝试分配它。

你的提交将检查并根据需要处理。

DOs
经常检查你提交的所有垃圾邮件或正常邮件 - 混合这些将使服务产生负面效果。

每隔 24 小时转发一次邮件至 RDP 监控团队 - 请只发送当前邮件。

超过一周的邮件可能已经被报告并服务已更新。

创建一个包含 X-CTCH 原始信头邮件的 ZIP 归档，并且保存在 **server/mail** 目录下的 EML 或 MSG 格式或 .imap/.tmp 文件复本。

准备两个单独的归档用于正常邮件误报和垃圾邮件误报。

在 zip 文件根目录下的 Zip 邮件不要设置密码保护。

为垃圾邮件误报 ZIP 文件命名为 FP.zip ，为正常邮件误报命名为 FN.zip 。

信息终端用户被收到且在任何流行邮件客户端包括爱思华宝 WebClient 内找到后应立即使用 另存为 功能保存为一个 raw 格式。

只有 EML 和 MSG 格式保留原始信头。

该文件可以作为附件发送且最后打包到 ZIP 文件。

信息保存在其他格式将被跳过并不被报告。

DO NOTs

如果原始邮件已经在终端用户和你之间转发或重定向，即使报告给我们也是毫无用处。.

当收到时立即保存他们为 EML 或 MSG 并把这些文件作为附件发送是非常必要的，否则原始信头信息将丢失且错误类别不能报告。

转发或者重定向该邮件到地址将被拒绝。

发送一个邮件并嵌入该信息(没有打包至一个 ZIP 文档) 或使用错误的密码将被忽略。

不要提交不包含 X-CTCH 信头的邮件。

不要提交正常爱思华宝反垃圾邮件误报/负数，邮件没有 X-CTCH 信头将被跳过且无论如何不会报告。

报告邮件地址

提交邮件相应语言的报告至国家/地区合伙人，例如 ***aslive-genuine@icewarp.fr*** 如果邮件是法语。

分公司将检查提交(不混合 FP 和 FN)并转发它们给爱思华宝总部，汇总后联系 RDP 服务监控程序团队并更新到服务器提供工作。

这些步骤是必需的以确保提交的正确性。

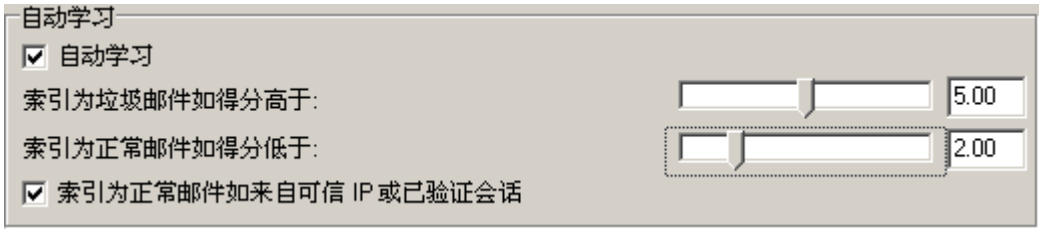
如果没有与你的语系有关的分公司，包含这两个文件(FP.zip 和 FN.zip)的邮件可以直接发送至 ***support@icewarp.com*** 或提交到支持中心，支持工程师将检查格式的正确性。

注意：发送至 ***support@icewarp.com*** 的邮件应该使用英文书写，否则将被忽略(除非另有约定)。

反垃圾 - 贝叶斯

贝叶斯过滤器是一个种识别垃圾邮件的统计方法。可建立词库，并通过识别关键字在垃圾邮件与有害邮件中出现的频率，来识别一条包含此关键字的邮件为垃圾邮件的可能性。

字段	描述
激活	激活使用贝叶斯过滤器。推荐使用此选项。
优化贝叶斯数据库	按下按钮，删除出现频率较低的词语。这些词语大多为垃圾邮件中经常看到的任意词语。 压缩数据库后，由于这些低频率词语已被删除，贝叶斯过滤器的精确度会增加。 此按钮仅将用户参考库进行压缩。



字段	描述
自动学习	此选项用于启用爱思华宝服务器的贝叶斯自动学习功能。 若邮件的垃圾邮件得分处于设定范围之内，则邮件将自动被标记出并添加至用户参考库中。
索引为垃圾邮件如得分高于	可通过移动滑动块设定分值。 分数等于或高于此分值的任何邮件将被索引为垃圾邮件。
索引为正常邮件如得分低于	可通过移动滑动块设定分值。 分数等于或低于此分值的任何邮件将索引为正常邮件。
索引为正常邮件如来自可信 IP 或已验证会话	选择此选项后，若邮件来自信任的 IP 地址或被允许的会话（即，允许 SMTP 的外发会话、允许 SMTP 之前的 POP 信，或来自信任的 IP 地址），则会被标记为合法信息。

字段	描述
忽略词	包含了在垃圾邮件参考库更新（标记过程）中将忽略的词语。我们强烈推荐将内部通讯中常用的词语添加进去，如公司名称、产品、服务等。

本章内容

贝叶斯过滤器 - 基本概念.....37

贝叶斯过滤器 - 基本概念

由于在爱思华宝服务器内执行，贝叶斯过滤器使用两个参考数据库决定一封邮件成为垃圾邮件可能性的大小：

参考数据库，通过使用现实邮件在现实邮箱管理系统上建立并提供使用。通过反垃圾邮件更新功能可对数据库进行更新。

爱思华宝通过自动学习功能与/或索引关键词功能建立的用户参考数据库。通过服务器的实际邮件，对每个安装的反垃圾功能来说变得更加具体和有针对性，个性化更强。

用户参考数据库信息高于参考数据库信息，自动完善，自动提高和改进。

贝叶斯过滤器是基于贝叶斯可能性理论而工作的。

根据贝叶斯基本理论，一些事情将要发生的可能性与过去已经发生的可能性是相同的。对于它们来说，如果要精确运行，应选择适合的垃圾邮件与合法（ham）信息进行分析。

在爱思华宝服务器内的执行过程如下：

找出一条垃圾信息包含某一特定词语的可能性大小。

乘以任何邮件为垃圾邮件的可能性。

除以合法信息中含有特定词语的可能性。

得出信息为垃圾邮件的可能性。

举例

假设：

我们共接收并分析了十万封邮件。

其中，八万封邮件为垃圾邮件。

四万八千封垃圾邮件包含词语 **viagra**。

四百封合法邮件中包含词语 **viagra**。

然后：

则垃圾邮件包含词语 **viagra** 可能性为 48,000/80,000=0.6

一封邮件为垃圾邮件的可能性为 80,000/100,000=0.8

任何邮件包含词语 **viagra** 的可能性为(48,000+400)/100,000=0.484

因此根据贝叶斯理论，包含词语 **viagra** 的邮件为垃圾邮件的可能性为 0.6*0.8/0.484=0.991

这也说明，包含词语 **viagra** 的信息为垃圾邮件的可能性为 99.1%

我们推荐最初进行为期两周的自动学习期限，且至少每 3-4 月进行一次压缩与重新学习。这就允许用户参考数据库随着公司信息内容的更改进行更新（例如，公司开始出售债券）。

用户参考数据库最大可包含十万个词语。你可以看到总体标签中实际存储的词语数。

一旦达到存储极限，则对数据库进行压缩（删除低频率、非重要的词语），并再次激活自动学习的特性。

参考数据库包含在文件<IceWarp directory>/spam/spam.db 中。

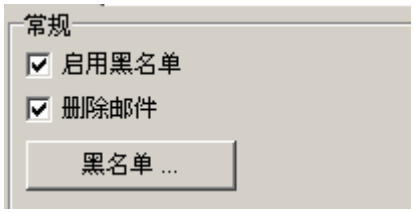
用户参考数据库包含在文件<IceWarp directory>/spam/spam.usr 中。

反垃圾 - 黑白名单

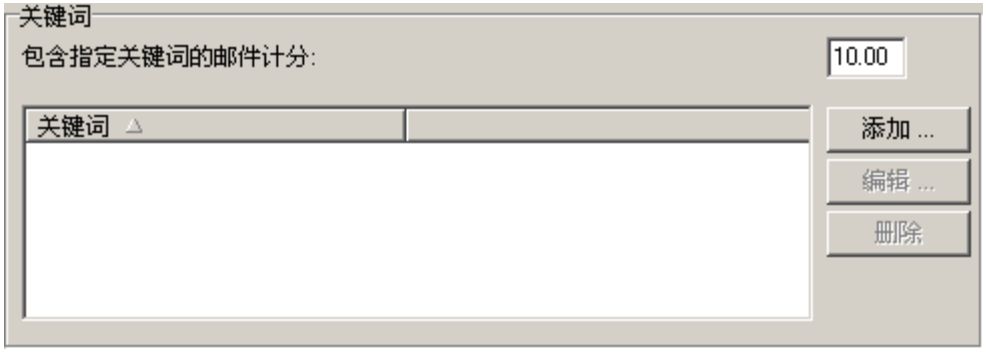
本章内容

黑名单 39
白名单 40

黑名单



字段	描述
激活黑名单	此选项用于启用黑名单处理功能，对邮件的垃圾分数进行修改。 注意：如果您启用隔离区，黑名单和白名单将同时启用。随着隔离区的启用，这些选项将不能被禁用。
删除邮件	此选项用于当邮件分数超过值即删除邮件。
黑名单	按下此按钮即可跳至垃圾邮件黑名单队列中。



黑名单关键词 部分允许你定义一个词语列表，如果发现一封邮件中有这些关键词，邮件的计分将上升。

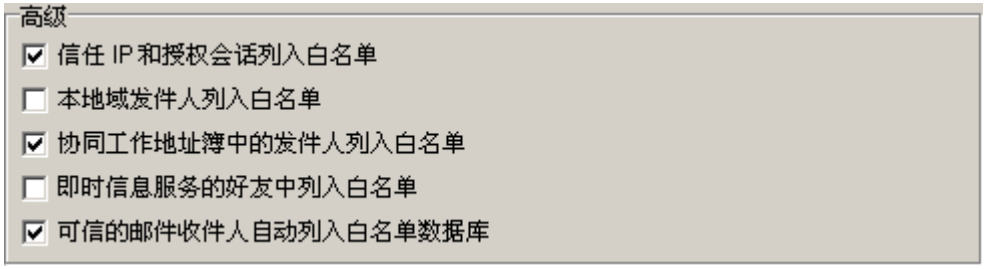
字段	描述
包含指定关键字的邮件计分	输入一个值以修改计分。
添加	按下按钮，将词语添加至列表。

编辑	按下按钮，修改所选词语。
删除	按下按钮，删除列表中的词语。

注意：某些情况下，爱思华宝服务器自动回复邮件给他们的发件人。例如自动回复，挑战响应，退信邮件等。这能确定发件人是一个正常人或一个垃圾发送者。

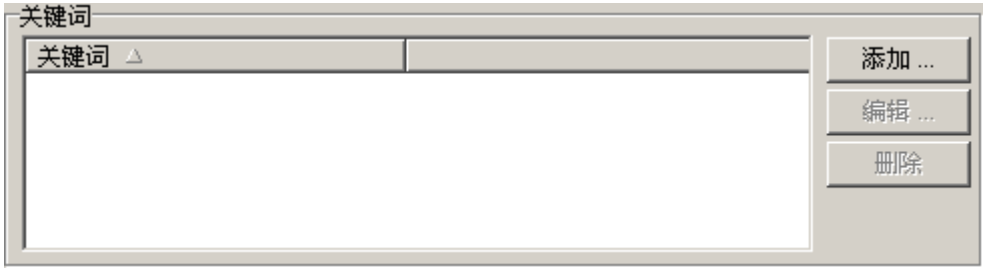
白名单

字段	描述
激活白名单	选择此按钮，使用反垃圾邮件白名单处理功能。 注意：如果您启用***隔离区***，***黑名单***和***白名单***将同时启用。随着***隔离区***的启用，这些选项将不能被禁用。
白名单	按下此按钮转至垃圾邮件队列节点，并选择***白名单***。



字段	描述
信任 IP 和授权会话列入白名单	此选项用于将信任列表中的 IP 地址自动添加至白名单中。 也可将经鉴定的会话项添加至白名单。. 注意：IP 地址将白名单但不增加到数据库。
本地域发件人列入白名单	此选项用于将来自于本地域的 ***发送者*** 添加至白名单中。 注意：发件人执行白名单动作但不增加至数据库。
协同工作地址簿中的发件人列入白名单	选择此选项，则爱思华宝自动将群地址簿中的地址添加至白名单中。 注意：发件人执行白名单动作但不增加至数据库。
即时信息服务的好友列入白名单	选择此选项，则爱思华宝自动将任何即时信息名单中的地址添加至白名单中。 注意：发件人执行白名单动作但不增加至数据库。

可信的邮件收件人自动列入白名单数据库	此选项用于将受信任的邮件地址添加至白名单数据库中。



白名单关键字部分可允许你对一系列的词语/短语进行定义，若一条信息中出现所定义的词语/短语，则信息可以绕过反垃圾邮件处理。

字段	描述
添加	按下按钮，将词语/短语添加至列表。
编辑	按下按钮，修改所选词语。
删除	按下按钮，删除列表中的词语/短语。

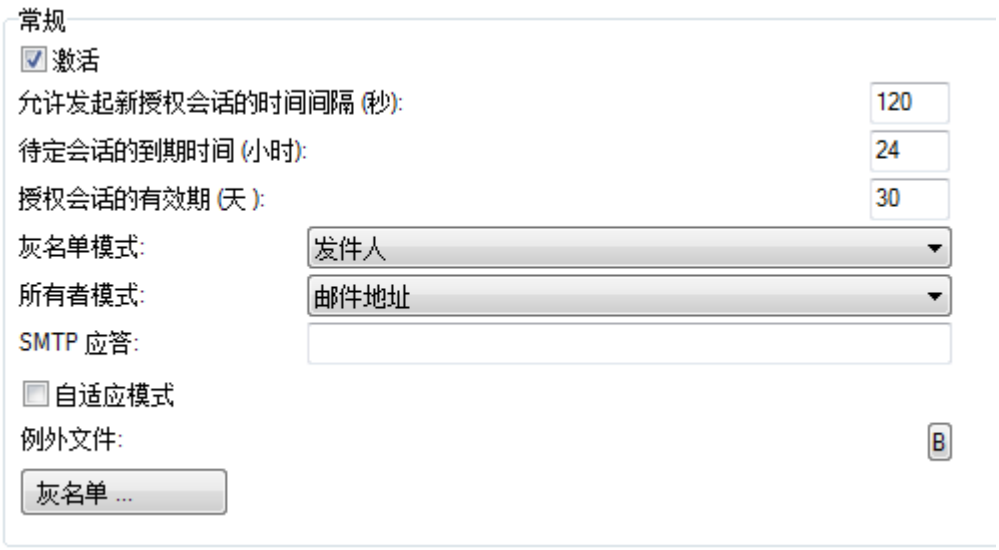
注意：自动白名单条目没有显示的标志，只是在 ***sndIP*** 列有一些区别（SQL 管理器 -- antispam.db）。自动白名单条目的该字段将有一个 IP 地址值，而白名单记录因手工被添加（通过 WebClient 或控制台），所以该字段为空。

因此，例如 ***DELETE FROM Senders WHERE SndIP*** !=''; 命令 将删除所有自动白名单的记录。（使用该方法前请备份你的 DB）。

灰名单

大多数的垃圾邮件制造者服务器会尝试向接收服务器发送邮件，如短期内未得到回应，则放弃。而真正合法服务器则会在一段时间后重新试着建立会话。

灰名单允许你设定拒绝接收到的会话的期限。此功能将阻止很多垃圾邮箱管理系统发送的邮件。



注意：本地忽略对于灰名单来说很重要。Bypass trusted IPs,

忽略受信任的 IP 地址，

本地 本地忽略过滤器。

灰名单忽略文件（greylist.dat）

如果未应用，用户将在邮件客户端中收到临时错误 4.5.1，并可在 x 秒后发送信息。.

字段	描述
激活	此选项用于启用灰名单功能。
允许发起新授权会话的时间间隔 (秒)	设定拒绝接收连接的时间。在这段时间内任何重新连接都将被拒绝。
待定会话的到期时间 (小时)	设定一段时间，在此时间后任何解决 IP 地址都将从数据库中删除。 待决 IP 地址指的是那些试图进行连接但被灰名单拒绝的地址。
授权会话的有效期 (天)	设定被授权 IP 地址在数据库中保留的天数。 若设定天数为 0，则被授权的 IP 地址将永远不会被删除。

	授权地址指的是被灰名单拒绝，但重新连接时被接受的地址。
灰名单模式	选择应该存储在灰名单数据库中的数据。 有四种模式可供选择： ▪ **发件人** 电子邮件发送者的邮件地址。 ▪ **IP -** 发送电子邮件的机器的 IP 地址。 ▪ **Sender&IP -**包含以上两种情况。 ▪ **IP+HELO/EHLO -** 发送电子邮件的机器的 IP 地址，与 SMTP 会话初期时 HELO/EHLO 命令发送的主机名。 注意：推荐使用 发件人 模式。 多 IP 系统，如 gmail，可能会从不同 IP 地址进行重新连接，这会使其依次被列入灰名单中。
所有者模式	从以下两项中选择： **邮件地址** 选择此项将灰名单与单个邮件地址建立关联。一封邮件一旦通过类名单，也只有收件人以后可以不通过灰名单检查而直接接收该邮件。 **域名** 选择本项后，灰名单将与整个域关联，一旦邮件通过灰名单的审核，整个域将可收到该邮件发件人发出的邮件。
SMTP 应答	如果你愿意，可对灰名单拒绝连接时作出的 SMTP 响应进行自定义。 如果不进行设定，则返回默认的 SMTP 响应信息。
自适应模式	如果启用，它将改变发件人的灰名单的状态。 如果一个发件人发送的邮件，最终被判断为垃圾邮件，灰名单将对该发件人重新打开，因此来自该发件人的邮件下次将重新被灰名单。
例外文件	按下 B 按钮编辑灰名单迂回文件，可设定不会被列入灰名单中的用户、域与 IP 地址范围。 文件中已给出具体例子。
灰名单	按下此按钮即可跳至垃圾邮件灰名单队列中。

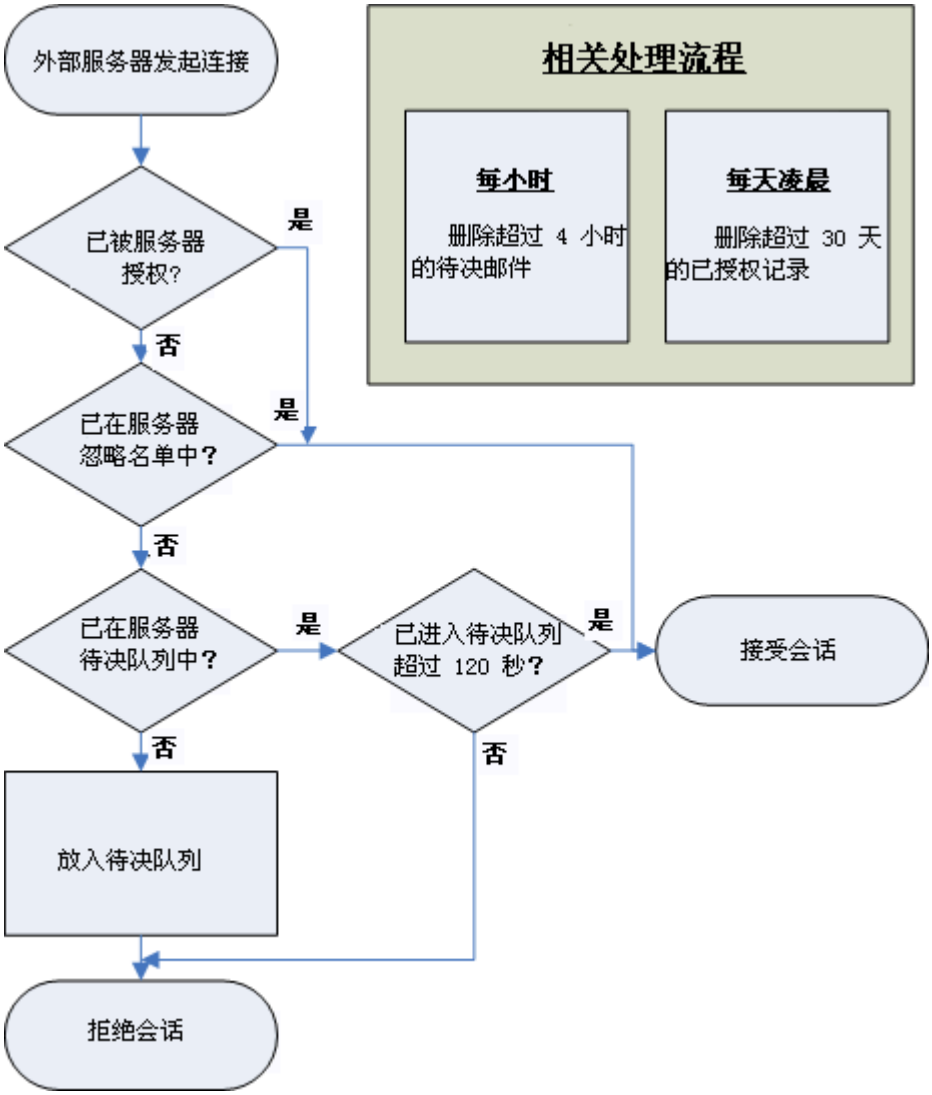
本章内容

灰名单流程图.....43

灰名单流程图

下面的流程图对灰名单如何工作进行了解释。

此流程图不是代码的准确呈现，而仅仅是一个工作原理的视图指导。



反垃圾 - 学习规则

由于垃圾邮件制造者的技术一直在不断进步，有时会发生垃圾邮件被错误判断为合法邮件的情况，或者极少数情况下合法邮件被错误判断为垃圾邮件。

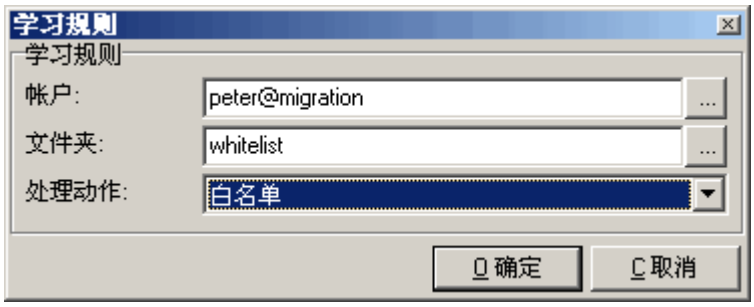
学习规则允许让用户自动解决这些问题，对错误识别的信息标定指数，或将信息的发送者添加至黑名单或白名单中。

队列可以是

- 通过帐户名识别的邮箱文件夹
- 任何 IMAP 文件夹

邮件会被复制或移动到相关地方。

按钮	**描述**
添加	点击按钮创建一个新的规则。 **学习规则** 对话框将打开。
编辑	选择规则并点击按钮进行编辑。 **学习规则** 对话框将打开。.
删除	选择一个规则并点击按钮删除规则。
立即处理	邮件将在凌晨进行处理。 点击该按钮将立即处理邮件。
设置文件	点击按钮在一个文本编辑器中打开设置文件。 你将看到所有已创建规则并可以使用正确语法创建更多规则。 在编辑器内点击 ***Comment*** 按钮打开一个语法说明的信息面板。



字段	描述
帐户	若队列基于邮箱文件夹，在此处输入帐户。 按下 ？，打开标准的选择项对话框。 警告 - 索引完成后，此邮箱的所有邮件会被删除。建议使用单独的邮箱文件夹来索引，要么复制（正常邮件）或移动（垃圾邮件）到该文件夹。
文件夹	若队列基于 IMAP 文件夹，在此处输入文件夹名。 按下 ？，打开一个标准的对话框，转至目标文件夹。 警告 - 索引完成后，该 IMAP 文件夹的所有邮件会被删除。建议使用单独的 IMAP 文件夹来索引，要么复制（正常邮件）或移动（垃圾邮件）到该文件夹。
处理动作	从下拉框中选择队列类型。 **黑名单** -队列中包含的邮件其发送者应被列入黑名单。 **白名单** -队列中包含的邮件其发送者应被列入白名单。 **贝叶斯 - 添加 - 垃圾词** -邮件内容索引为垃圾词。 **贝叶斯 - 添加 - 正常词** -邮件内容索引为正常词。 **贝叶斯 - 更改 - 垃圾词 -> 正常词** -此队列用于重新索引出于某种原因被误索引为垃圾词的邮件。该邮件的内容将被取消索引为垃圾词而索引为正常词。 **贝叶斯 - 更改 - 正常词 -> 垃圾词** -此队列用于重新索引出于某种原因被误索引为正常词的邮件。该邮件的内容将被取消索引为正常词而索引为垃圾词。 注意 为使黑名单功能正常作用，应激活此功能（参见 AS 白名单）。 将多个队列设定为同一种队列类型也是有效的。

推荐使用共用 IMAP 文件夹，这样用户可以直接在 Outlook 中看到队列，并可将需要标定指数的信息直接从客户端复制到队列中。

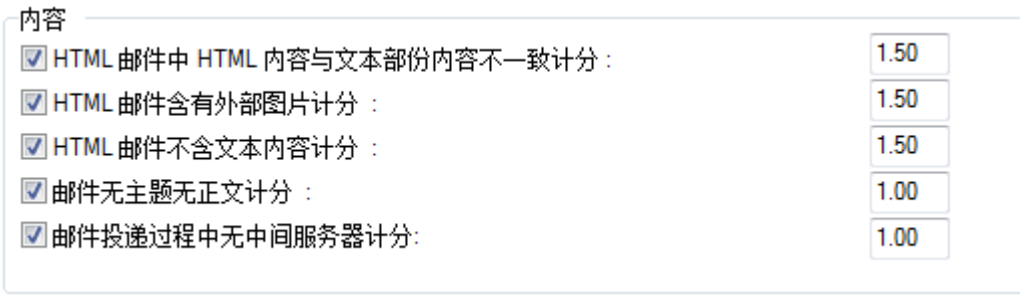
其他

本章内容

内容 47
字符集 48
发送者 48

内容

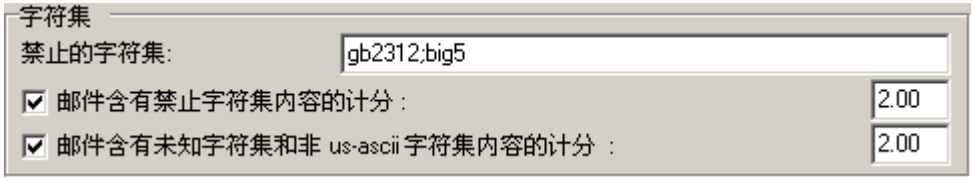
内容过滤器的收集功能已经被开用于获取最常见的垃圾邮件信息，这些邮件通常格式错误，或在服务器被破坏发送至多个收件人，或内容结构与典型的由普通邮件客户端发出的普通邮件完全不同。



选择一个选项，并输入数值。若测试结果为真，则将所输入数值添加至垃圾邮件分数。

字段 s	描述
HTML 邮件中 HTML 内容与文本内容不一致计分	如果邮件含有 HTML 及普通文本部分，则两部分应相匹配。很多垃圾邮件都包含这两个部分，但却不能相匹配。 选择此选项，使爱思华宝增加此类信息的垃圾邮件分数。 注意 一些邮件客户端不能正确生成普通文本部分，因此应小心,使用此选项，尤其在检查外发邮件时。
HTM L 邮件含有外部图片计分	对于普通邮件来说，含有连接至外部图像的链接是不正常的。
HTML 邮件不含文本内容计分	HTML 邮件应当有一个文本部分。
邮件无主题无正文计分	普通邮件应至少含有一个主题或部分邮件内容。
邮件投递过程中无中间服务器计分	普通邮件试图通过中间服务器进行发送(如,它们的网络服务提供商的服务器或公司服务器)

其他 - 字符集

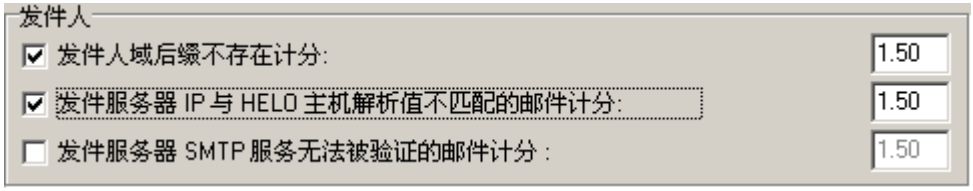


字段	描述
禁止的字符集	指定你认为可能是垃圾邮件的字符集列表。
邮件含有禁止字符集内容的计分	对于那些含有列表中任何字符集的信息，此选项可使爱思华宝服务器增加其垃圾邮件分数。 垃圾邮件分数增加的数值即为所设定的分值。 下表列出了更多的普通字符集。
邮件含有未知字符集和非 us-ascii 字符集内容的计分	对于那些含有失踪字符集或非 us-ascii 字符的信息，此选项可使爱思华宝增加其垃圾邮件分数。

重要提示

如果从一个网站通过爱思华宝服务器发送 HTML 形式的邮件，应注意这些信息通常包含高数值的字符（例如，一些外国姓名）。应牢记通过正确定义的字符集对信息进行构建，并将网站 IP 地址列入信任者名单。

发件人



字段	描述
发件人域后缀不存在计分	此选项用于爱思华宝服务器检查发送方的域名是否存在。 如果不存在，则爱思华宝服务器会增加垃圾邮件分数，增加值即为所设定的数值。
发件服务器 IP 与 HELO 主机解析值不匹配的邮件计分	此选项用于爱思华宝服务器检查 HELO 命令中的主机名解析相同的 IP 地址，此 IP 地址应为发送信息所在的地址。 如果不解析，则爱思华宝服务器会增加垃圾邮件分数，增加值即为所设定的数值。
发件服务器 SMTP 服务无法被验证的邮件	此选项用于使爱思华宝服务器验证发出邮件的 IP 地址为合法的 SMTP 服务器。 如果不合法，则爱思华宝服务器会增加垃圾邮件分数，增加值即为所设定的数值。

计分	警告 通过连接到邮件发送服务器的端口 25（标准 SMTP 端口）实现此功能。此功能的响应时间可高达 5 秒，因此会使服务器的速度变得非常慢。

反垃圾模板

在所有的反垃圾邮件界面，你都可以看到复原按钮。

可从下拉框选择高、中或低的反垃圾邮件模板设置，再按下复原按钮更改等级。

AntiSpam Level	描述
低级	反垃圾邮件的非常低的等级设置。 不使用灰名单功能。 不使用隔离功能。 垃圾邮件归类分数较高。 不使用发送者技术。 不使用垃圾邮件刺客 SPF、Razor2 与域钥匙功能。 此模板为资源最低模板，相比其他设置，能捕捉到的垃圾邮件相对较少。
中级	激活灰名单功能。 激活隔离功能。 降低垃圾邮件归类分数。 使用发送者技术。 激活 SPF 技术。 推荐使用此选项。 附加的处理功能会占用更多的服务器资源，但也能更加准确地对垃圾邮件进行识别。
高级	非常严格的反垃圾邮件设置。 使用所有可能的技术。 降低垃圾邮件归类分数。 垃圾邮件分数调整的数值高于其他模板。 资源最低的模板，能最准确识别出垃圾邮件，但出错几率也较高。

规则自定义 -local.cf 文件

local.cf 文件可用于自定义规则，比如设置相应 .cf 文件的默认值(<install_dir>/spam/rules)。.

不要修改这些文件，因为下次更新将会覆盖您的修改。

通过 local.cf file 的相应位置你可以例如重定义默认分值（对于一些技术），比如一些值过低或未被设置。

示例

DKIM

常用于白名单 Facebook, Twitter, LinkedIn updates。

注意： 反垃圾 ?垃圾杀手 ?使用 DKIM 选项启用 "DKIM" 功能使其工作。

最初，来自 rules/25_dkim.cf 文件的得分钟将被应用。

相关部份看起来如下：

header DKIM_VERIFIED eval:check_dkim_verified()

describe DKIM_VERIFIED Domain Keys: signature passes verification

score DKIM_VERIFIED -0.500

你可以复制 ***score DKIM_VERIFIED -0.50*** 行，粘贴到 ***local.cf*** 文件并改变该值，比如说 ***-1.000***

DNSWL

请首先启用 ***反垃圾 - 垃圾杀手-RBL*** ， "check_rbl_sub" 功能将工作。

添加这些行，local.cf 文件将工作：

header __RCVD_IN_DNSWL eval:check_rbl('dnswl-firsttrusted', 'list.dnswl.org.')

header RCVD_IN_DNSWL_LOW eval:check_rbl_sub('dnswl-firsttrusted', '127.0.\d+.1')

describe RCVD_IN_DNSWL_LOW Sender listed at http://www.dnswl.org/, low trust

tflags RCVD_IN_DNSWL_LOW nice net

header RCVD_IN_DNSWL_MED eval:check_rbl_sub('dnswl-firsttrusted', '127.0.\d+.2')

describe RCVD_IN_DNSWL_MED Sender listed at http://www.dnswl.org/, medium trust

tflags RCVD_IN_DNSWL_MED nice net

header RCVD_IN_DNSWL_HI eval:check_rbl_sub('dnswl-firsttrusted', '127.0.\d+.3')

describe RCVD_IN_DNSWL_HI Sender listed at http://www.dnswl.org/, high trust

tflags RCVD_IN_DNSWL_HI nice net

score RCVD_IN_DNSWL_LOW -1

score RCVD_IN_DNSWL_MED -10

score RCVD_IN_DNSWL_HI -100

反垃圾 - 垃圾邮件队列

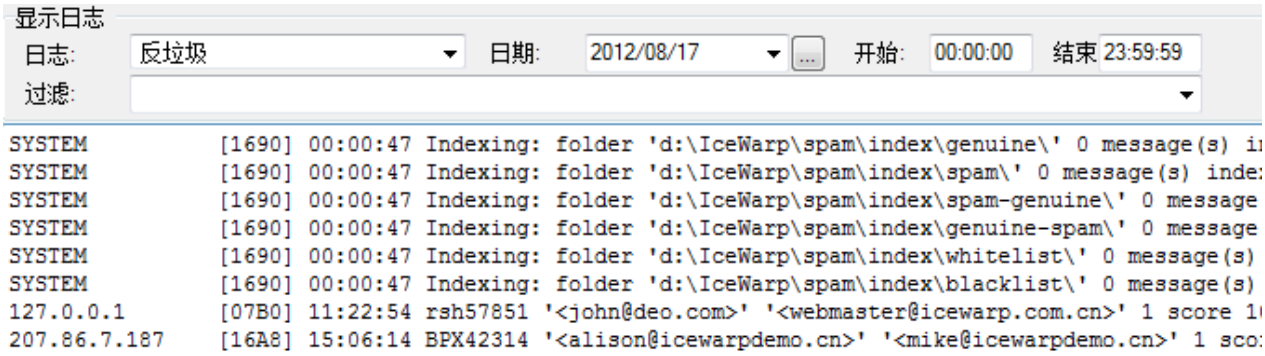
该节详细的信息，参考 **状态 - 垃圾邮件队列** 章节。

反垃圾 - 日志

如果已设置反垃圾邮件日志选项，可浏览反垃圾邮件日志查看遇到的问题，为什么会标记为垃圾邮件或者不被标记。

通过管理员控制台 系统->服务节点激活日志功能。请参考 系统 --服务 -- 常规 章节。

你可以通过 **状态 -- 日志** 节点查看反垃圾日志， 从相应列表选择 **反垃圾 和 日期** 。更多详细内容请参考 **状态 -- 日志** 部份。



上面的屏幕截图并未包含实际的日志信息，但我们可以通过一些例子讨论日志中一些内容的含义。

举例 1

127.0.0.1 [07B0] 11:22:54 RSH57851 '<john@doe.com>' '<webmaster@icewarp.com.br>' 1 score 10.00 reason [SpamAssassin=10.00,Bayes=99.99,Body=PE] action SPAM

在本手册中行被分隔，但在日志屏幕中它将被显示在一行中，相应字段的阐述请见下表：

字段	描述
127.0.0.1	发送/接收此邮件时连接到爱思华宝服务器的 IP 地址。
[07B0]	为这个连接所分配的连接编号。
11:22:54	此日志项的时间戳。
RSH57851	邮件 ID。
'<john@doe.com>'	接收邮件的用户。
'<webmaster@icewarp.com.br>'	发送邮件的用户。
1	邮件接收者的数量。
score 10.00	此邮件的垃圾判断得分。 注意 - 这种评分最大值是 10。邮件得分超过 10 分，爱思华宝服务器自动将分值设为 10 分。

reason [SpamAssassin=10.00,Bayes=99.99,Body=PE]	SpamAssassin=10.00 - 垃圾杀手得分 4.39。 Bayes=99.99 - 根据贝叶斯过滤器，此邮件是垃圾邮件的概率。 Body=PE: ▪ P - HTML 与文本内容不一致(参见 **原因码**)。 ▪ E - 邮件含有外部图片(参见 **原因码**)。
action SPAM	这是根据垃圾邮件分数采取的行为 - 此邮件已被标记为垃圾邮件。 根据得分会有以下四个动作： ▪ SPAM - 邮件标记为垃圾邮件。 ▪ QUARANTINE - 邮件被隔离。 ▪ REFUSE - 邮件被拒绝。 ▪ NONE - 邮件被接收。

原因码

在邮件被标记为垃圾邮件以及忽略反垃圾邮件处理时，反垃圾邮件引擎会返加原因码。

共有四套逻辑代码 - 垃圾邮件原因码、字符集原因码、在线反垃圾原因码与忽略原因码，分别描述如下：

垃圾邮件原因码

问题代码	原因
P	HTML 与文本部分不匹配
E	内容中包含外部图像
N	无文本部分
I	内容中含有内嵌图像
B	无正文、无标题
R	无中间服务器
S	邮件中含有脚本
F	通过过滤器对垃圾邮件打分
K	通过黑名单关键字给垃圾邮件打分
X	邮件不能进入隔离区

字符集原因码

代码	原因
F	不允许的字符集
M	错误的字符集信息

忽略原因码

代码	原因
B	因为任何条目信息包含在忽略文件中，这包括发件人、收件人、本地发件人、信任会话等。
G	发件人包含在协同工作地址簿中
H	如果远程端告诉我们发送者是本地的，但未通过身份验证，也不是来自受信任的 IP，则白名单和黑名单被跳过，该邮件做为普通邮件处理 - 其他规则的应用。
K	发现包含在白名单关键字中的词语
L	许可证无效

M	由于为特定帐户设定了访问模式而此帐户不包含在其中，因此绕过垃圾邮件处理
O	外发信息
Q	本地域发送者 如果 - 如您想白名单/不白名单本域发送者，启用/禁用该选项点导航至 反垃圾/黑&白名单节点 / 白名单选项。
R	发件人在收件人 IM 联系人中
S	超过能检查的最大邮件
T	受信任的发送者
U	假如 垃圾邮件 文件夹或隔离报告的启用，所有来自本地或负载平衡方案中"友方? 服务器的爱 smtp 连接 的发件人与反垃圾/隔离区报告中设置的发件人比较，如果匹配，连接将被白名单，且忽略原因码 U 将出现。
W	发送者包含在白名单中， 或者一个规则接受该邮件
X	邮件由于一些原因不能被隔离，例如隔离未激活。 (查看 反垃圾 - 常规 - 常规 选项卡。)
J	收件人没有激活隔离选项 (查看 反垃圾 - 常规 - 常规 选项卡。)
Z	本地用户模式设置为不隔离 (查看 *反垃圾 - 常规 - 其他* 选项卡) 设置为 不隔离/白名单/白名单本地用户。

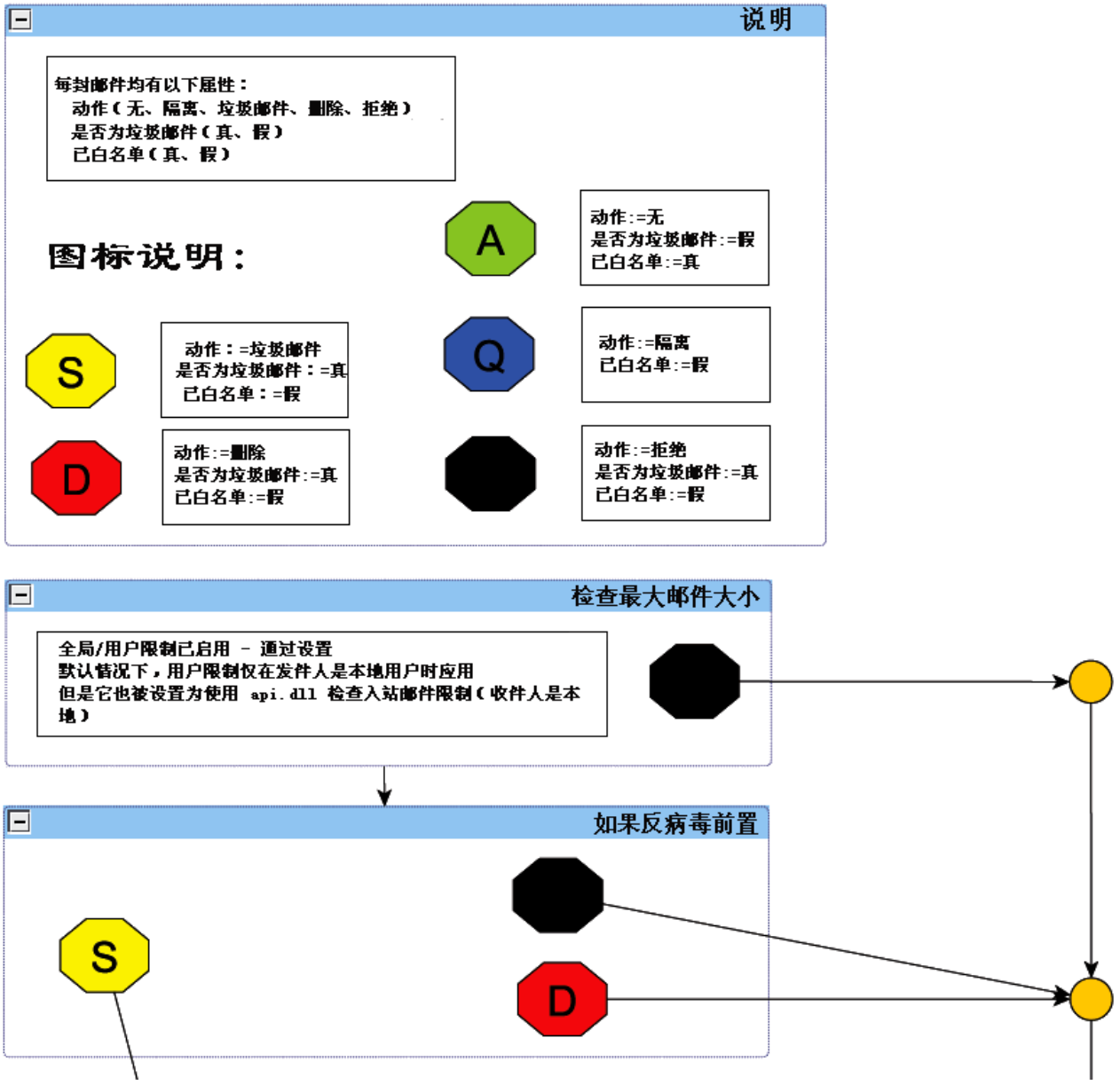
爱思华宝在线反垃圾原因

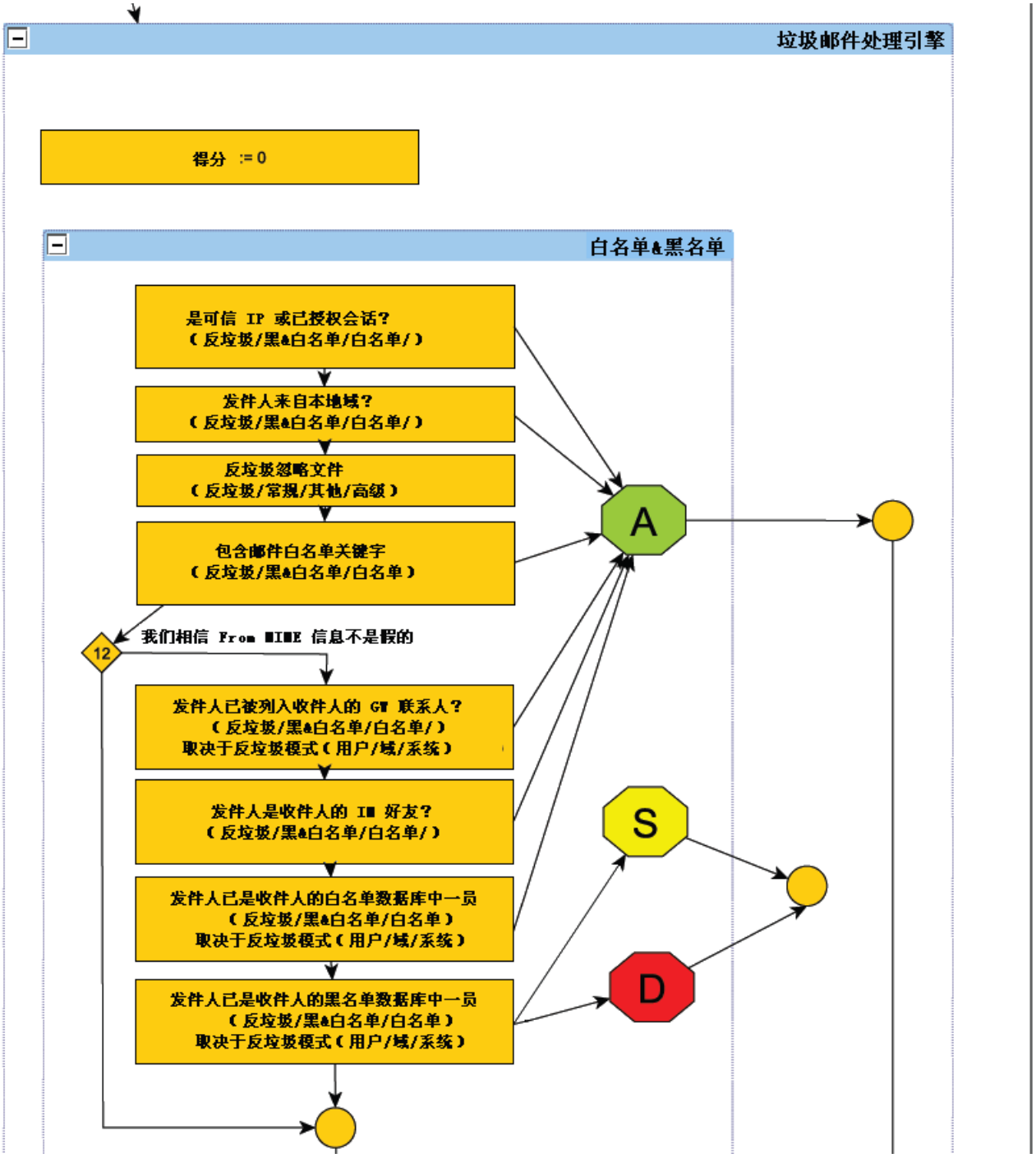
原因码	**原因**
Y	此邮件极有可能被标记为垃圾邮件。
H	此邮件标记为极有可能成为大量爆发的垃圾邮件。
N	

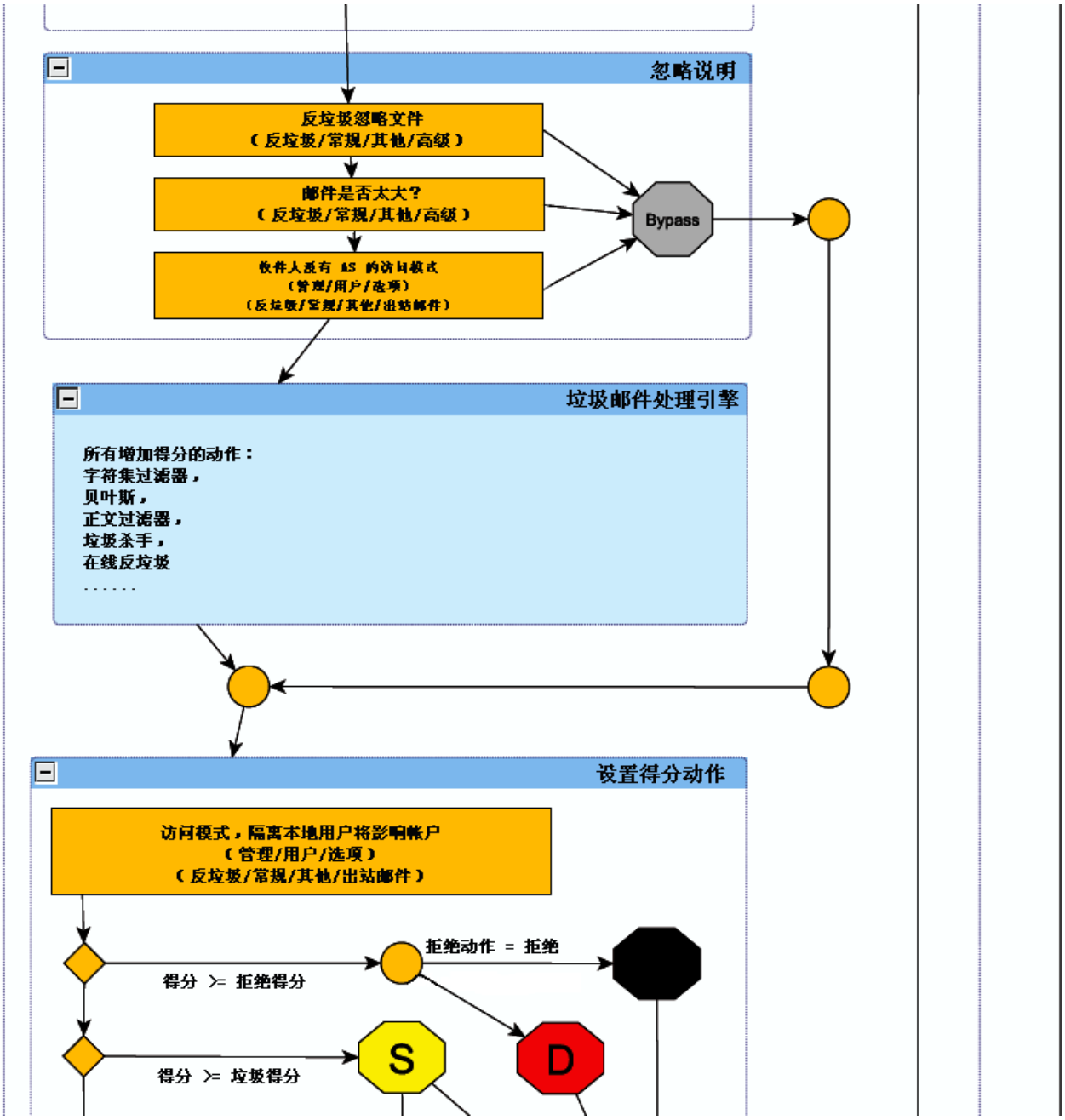
反垃圾流程图

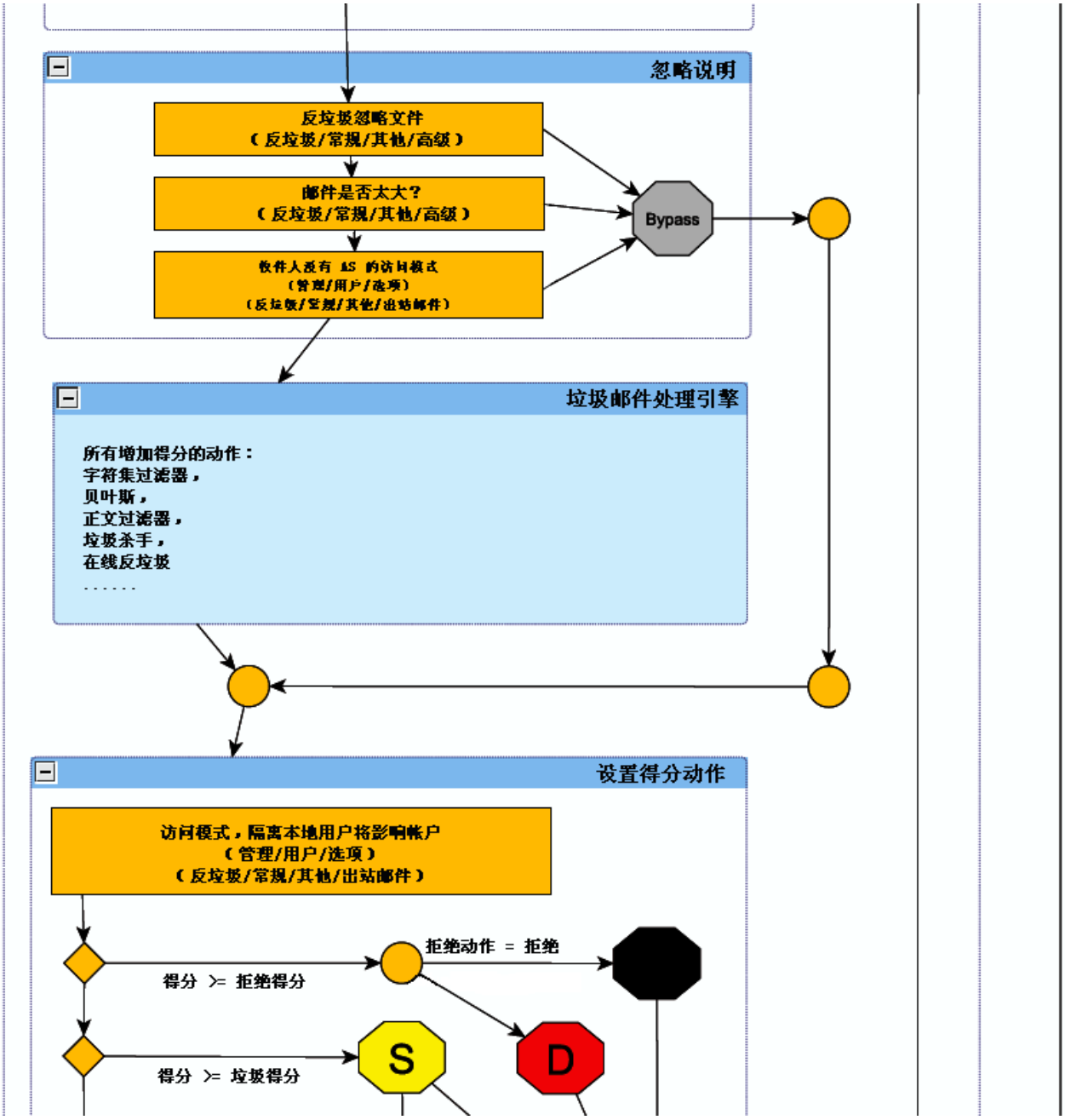
反垃圾：新的内部处理

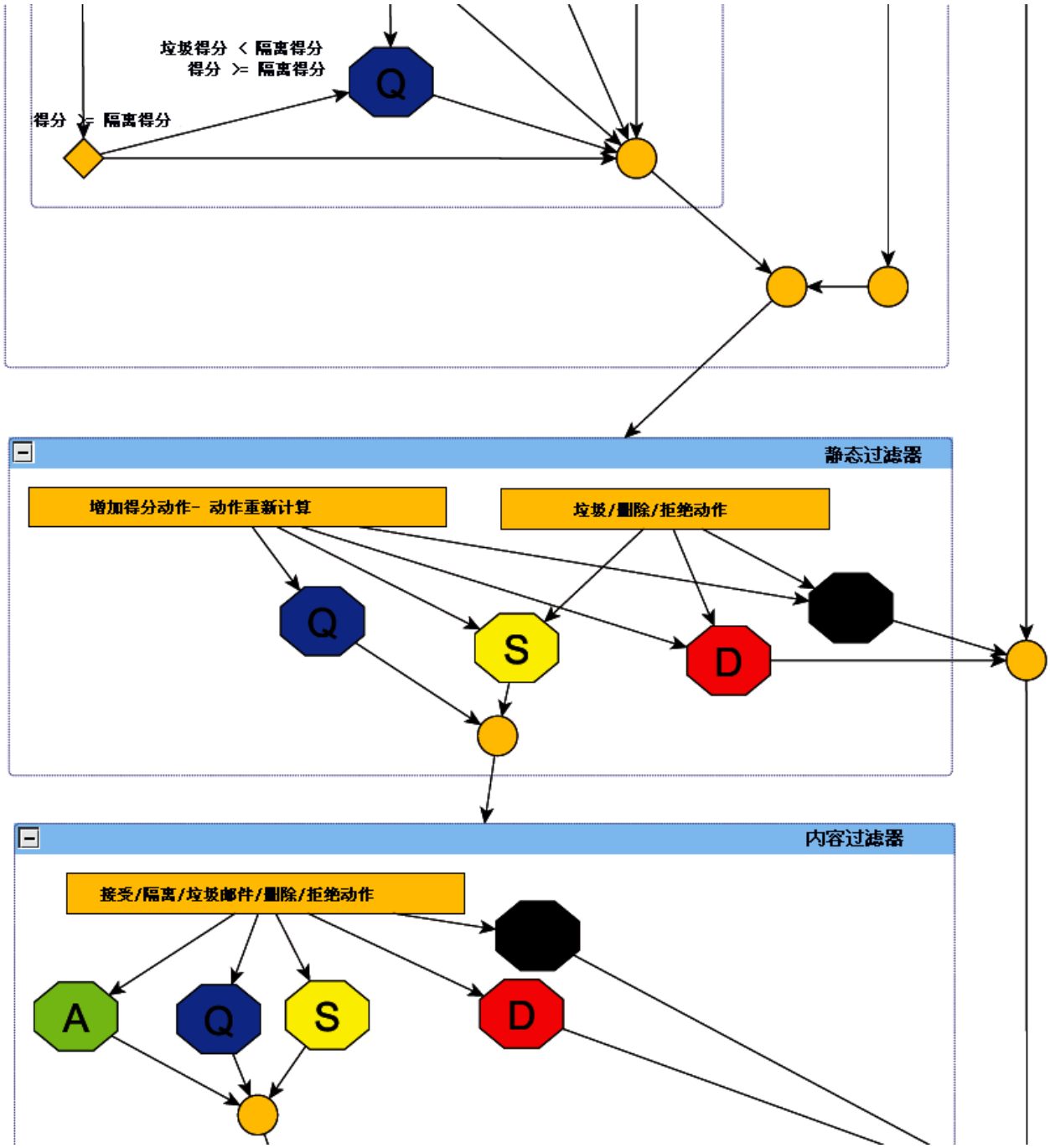
重新设计和文档化。解决所有已知问题包括忽略缺陷，访问模式，多个收件人问题，内容过滤器冲突等等。

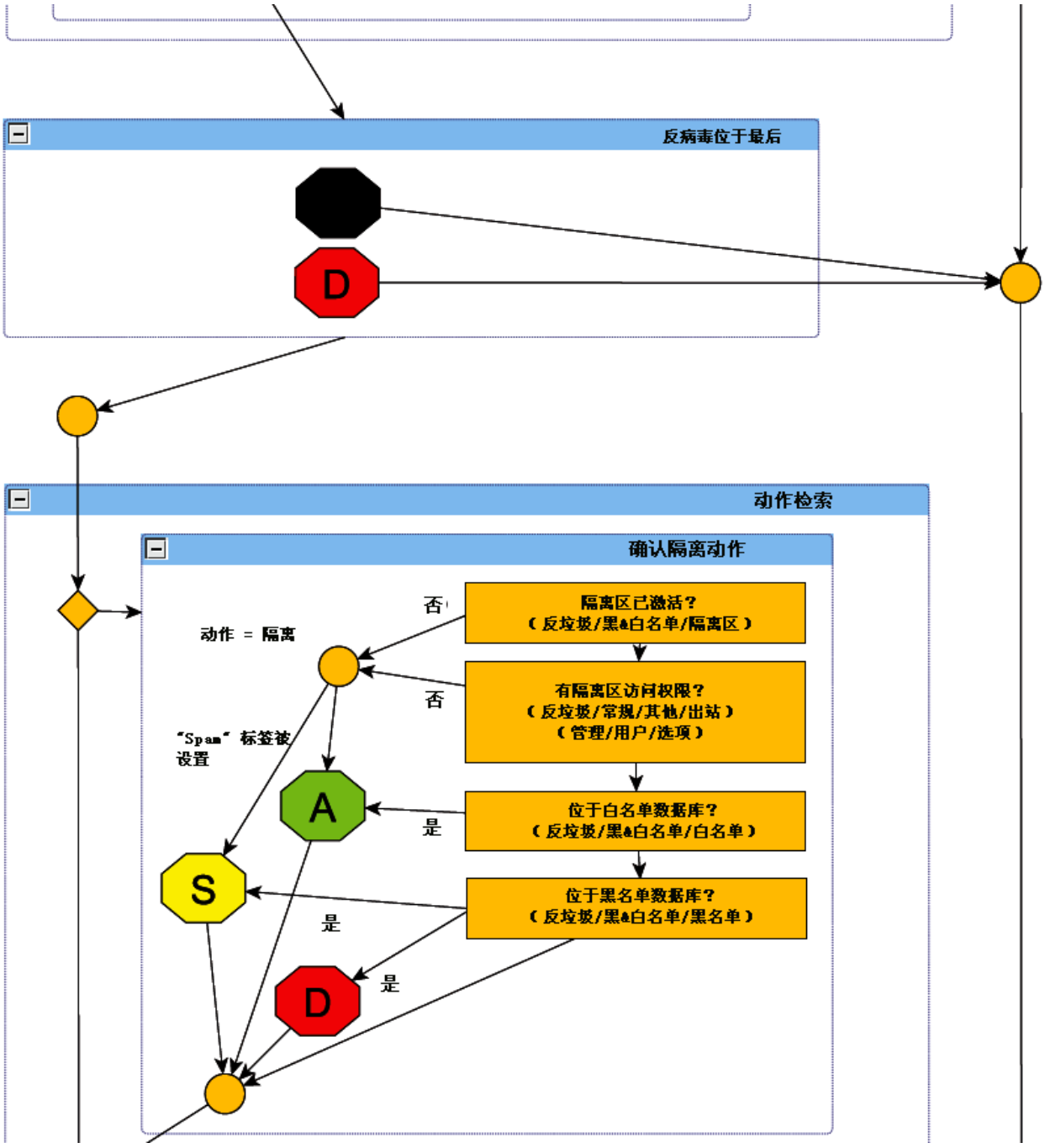


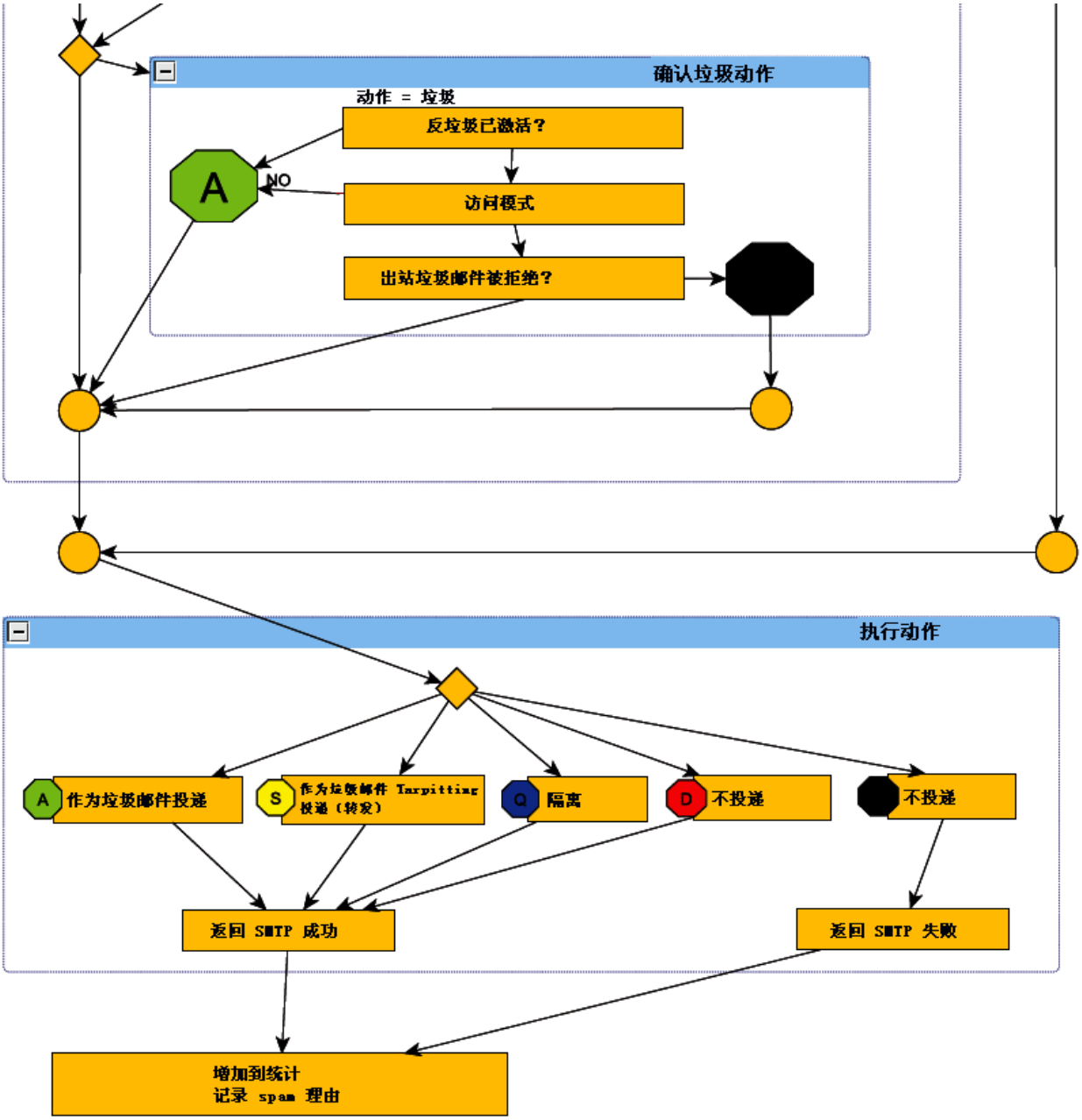

垃圾邮件处理引擎
得分 := 0
白名单&黑名单
是可信 IP 或已授权会话?
(反垃圾/黑&白名单/白名单/)
发件人来自本地域?
(反垃圾/黑&白名单/白名单/)
反垃圾忽略文件
(反垃圾/常规/其他/高级)
包含邮件白名单关键字
(反垃圾/黑&白名单/白名单)
我们相信 From MIME 信息不是假的
12
发件人已被列入收件人的 GW 联系人?
(反垃圾/黑&白名单/白名单/)
取决于反垃圾模式(用户/域/系统)
发件人是收件人的 IM 好友?
(反垃圾/黑&白名单/白名单/)
发件人已是收件人的白名单数据库中一员
(反垃圾/黑&白名单/白名单)
取决于反垃圾模式(用户/域/系统)
发件人已是收件人的黑名单数据库中一员
(反垃圾/黑&白名单/白名单)
取决于反垃圾模式(用户/域/系统)
A
S
D


忽略说明
反垃圾忽略文件
（反垃圾/常规/其他/高级）
邮件是否太大？
（反垃圾/常规/其他/高级）
收件人没有 AS 的访问模式
（管理/用户/选项）
（反垃圾/常规/其他/出站邮件）
Bypass
垃圾邮件处理引擎
所有增加得分的动作：
字符集过滤器，
贝叶斯，
正文过滤器，
垃圾杀手，
在线反垃圾
. . . . . .
设置得分动作
访问模式，隔离本地用户将影响帐户
（管理/用户/选项）
（反垃圾/常规/其他/出站邮件）
拒绝动作 = 拒绝
得分 >= 拒绝得分
得分 >= 垃圾得分
S
D


忽略说明
反垃圾忽略文件
（反垃圾/常规/其他/高级）
邮件是否太大？
（反垃圾/常规/其他/高级）
收件人具有 AS 的访问模式
（管理/用户/选项）
（反垃圾/常规/其他/出站邮件）
Bypass
垃圾邮件处理引擎
所有增加得分的动作：
字符集过滤器，
贝叶斯，
正文过滤器，
垃圾杀手，
在线反垃圾
. . . . . .
设置得分动作
访问模式，隔离本地用户将影响帐户
（管理/用户/选项）
（反垃圾/常规/其他/出站邮件）
拒绝动作 = 拒绝
得分 >= 拒绝得分
得分 >= 垃圾得分
S
D


垃圾得分 < 隔离得分
得分 >= 隔离得分
Q
得分 >= 隔离得分
静态过滤器
增加得分动作- 动作重新计算
垃圾/删除/拒绝动作
Q
S
D
内容过滤器
接受/隔离/垃圾邮件/删除/拒绝动作
A
Q
S
D


反病毒位于最后
D
动作检索
确认隔离动作
隔离区已激活？
（反垃圾/黑&白名单/隔离区）
否
动作 = 隔离
有隔离区访问权限？
（反垃圾/常规/其他/出站）
（管理/用户/选项）
否
"Spam" 标签被设置
A
位于白名单数据库？
（反垃圾/黑&白名单/白名单）
是
S
位于黑名单数据库？
（反垃圾/黑&白名单/黑名单）
是
D
是


确认垃圾动作
动作 = 垃圾
反垃圾已激活？
A
NO
访问模式
出站垃圾邮件被拒绝？
执行动作
A 作为垃圾邮件投递
S 作为垃圾邮件 Tarpitting 投递（转发）
Q 隔离
D 不投递
不投递
返回 SMTP 成功
返回 SMTP 失败
增加到统计
记录 spam 理由