CACTER 邮件安全云网关系统

管理员使用手册

文档更新

本文档由广东盈世计算机科技有限公司于2024年12月最后修订。

公司网站

https://www.cacter.com

销售咨询热线

400-000-1631

技术支持热线

400-888-2488

A、 文档修改记录

版本	修改日期	修改人员	修改记录
V1	2021-3-26	刘佳雄	创建文档
V1.1	2021-5-12	刘佳雄	更新产品功能
V1.2	2021-6-22	刘佳雄	更新产品功能
V1.3	2022-3-20	周婷	更新产品功能
V6.7.3.1	2022-9-27	唐雨晴	更新产品功能
V6.7.3.1.1	2022-12-2	唐雨晴	更新产品功能
V6.8.1	2023-6-19	唐雨晴	更新产品功能
V7.0.1.2	2024-6-13	陈皓隽	更新产品功能
V7.3.0.3.1	2024-12-2	陈皓隽	更新产品功能

B、 文档审核记录

版本	审核日期	审核人员	审核记录

目 录

目 录 3
1 前言 1
2 使用说明 1
3 登录/登出 2
4 功能详解 3
4.1 系统状态 3
4.2 过滤规则 6
4.2.1 发信 IP 过滤（路径：过滤规则-发信IP过滤） 6
4.2.2 IP 频率限制（路径：过滤规则-IP频率限制) 6
4.2.3 发信人过滤（路径：过滤规则-发信人过滤） 7
4.2.4 内容过滤（路径：过滤规则-内容过滤） 8
4.2.5 高级内容过滤（路径：过滤规则-高级内容过滤） 9
4.2.6 用户自定义规则（路径：过滤规则-用户自定义规则） 10
4.2.7 全局设置（路径：过滤规则-全局设置） 12
4.2.8 群组策略（路径：过滤规则-群组策略） 14
4.3 统计报表 16
4.3.1 邮件过滤统计（路径：统计报表-邮件过滤统计） 16
4.3.2 邮件类型统计 17
4.3.3 IP 链接统计（路径：统计报表-IP 链接统计） 17
4.4 日志查看 18
4.4.1 邮件投递日志（路径：日志查看-邮件投递日志） 18
4.4.2 恶意邮件日志（路径：日志查看-恶意邮件日志） 18
4.4.3 链接保护日志（路径：日志查看-链接保护日志） 19
4.4.4 管理员操作日志（路径：日志查看-管理员操作日志） 19
4.5 邮件隔离 19
4.5.1 邮件隔离区（路径：邮件隔离-邮件隔离区） 19
4.5.2 隔离区设置（路径：邮件隔离-隔离区设置） ..... **错误！未定义书签。**

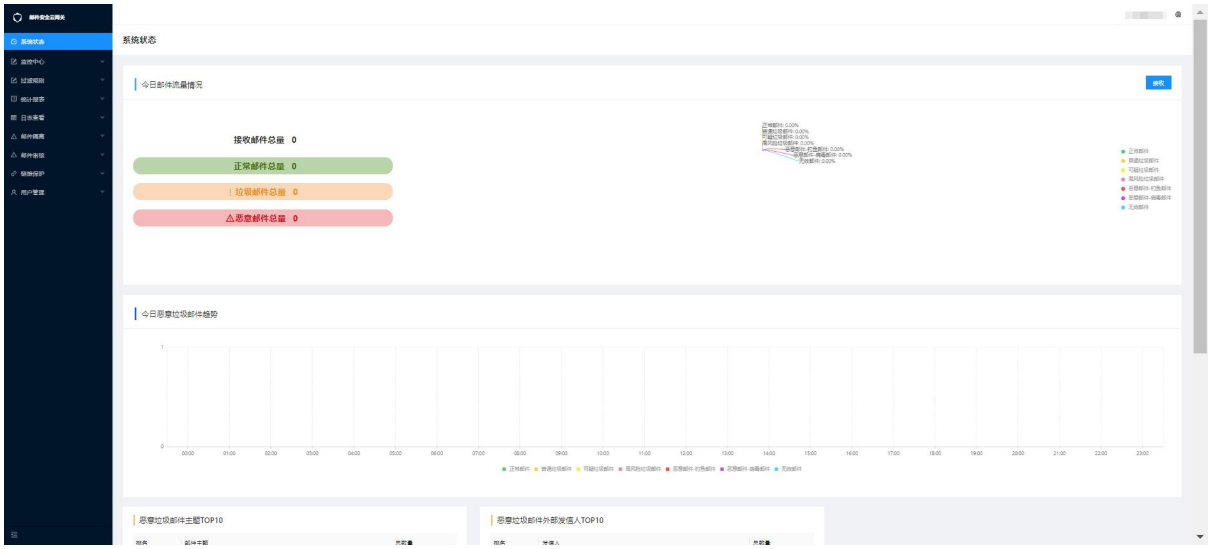
4.6 邮件审核 21
4.6.1 邮件审核队列（路径：邮件审核-邮件审核队列） 21
4.6.2 邮件审核日志（路径：邮件审核-邮件审核日志） 22
4.6.3 邮件审核设置（路径：邮件审核-邮件审核设置） 22
4.7 链接保护 23
4.7.1 链接保护统计（路径：链接保护-链接保护统计） 23
4.7.2 链接保护白名单（路径：链接保护-链接保护白名单） 24
4.8 用户管理 24
4.8.1 帐号安全（路径：用户管理-账号安全） 24
4.8.2 登录设置（路径：用户管理-登录设置） 25
4.8.3 管理员设置（路径：用户管理-管理员设置） 26
4.8.4 角色权限 （路径：用户管理-角色权限） 27
5 附件 27
附件一 垃圾邮件投递到邮箱垃圾邮件文件夹配置方法 27

1 前言

欢迎阅读《CACTER 邮件安全云网关系统 V7.3.0.3.1 管理员使用手册》。本手册包含有CACTER 邮件安全云网关系统的功能、系统要求的信息以及配置使用设置的相关说明。

2 使用说明

CACTER邮件云安全网关导航栏展示区如图（图1-1）包括系统状态、监控中心、过滤规则、统计报表、 日志查看、邮件隔离、邮件审核、链接保护、用户管理几大模块。



各模块二级功能菜单如下所示：

系统状态

1. 今日邮件流量情况
2. 今日恶意垃圾邮件趋势
3. 恶意垃圾邮件主题TOP10
4. 恶意垃圾邮件外发发信人TOP10

监控中心

1. 通知管理

过滤规则

1. 发信IP过滤
2. IP频率限制
3. 发信人过滤
4. 内容过滤
5. 高级内容过滤
6. 用户自定义规则
7. 附件过滤
8. 全局设置

9. 群组策略

统计报表

1. 邮件过滤统计
2. 邮件类型统计
3. TOP统计

日志查看

1. 邮件投递日志
2. 恶意邮件日志
3. 链接保护日志
4. 系统通知信日志
5. 管理员操作日志

邮件隔离

1. 邮件隔离区
2. 隔离区设置

邮件审核

1. 邮件审核队列
2. 邮件审核日志
3. 邮件审核设置

链接保护

1. 链接保护统计
2. 链接保护白名单

用户管理

1. 账号安全
2. 登录设置
3. 管理员设置
4. 角色权限

3 登录/登出

- **登录**

  您可以使用浏览器登录 https://gw.cacter.com 访问云网关管理后台。

  输入管理员用户名和密码，点击登录按钮进入管理界面。

- **退出登录**

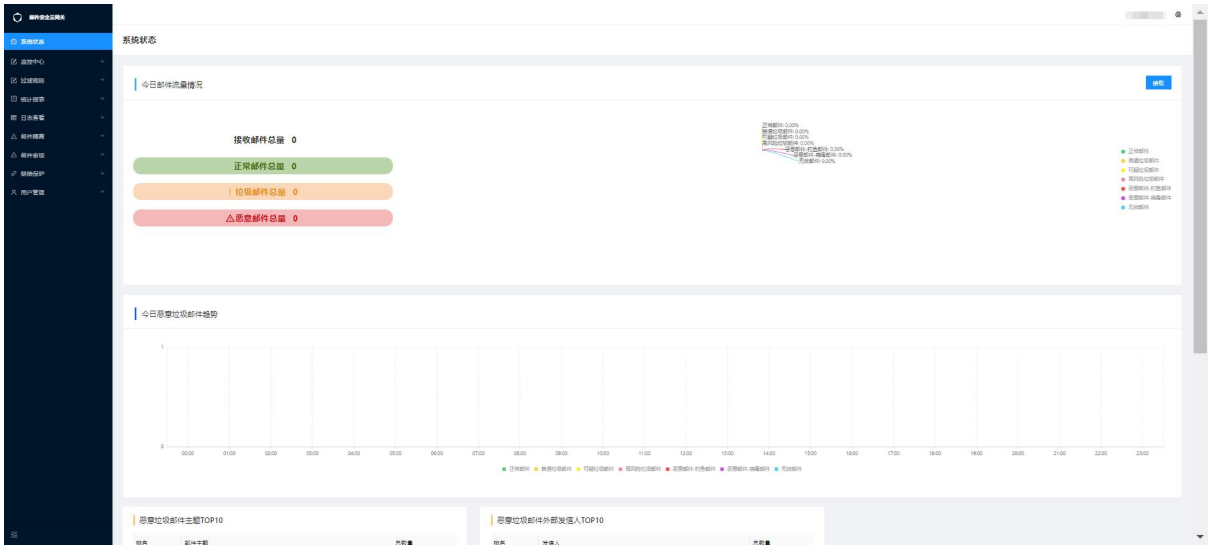
在管理页面右上方，系统提供了“退出登录”按钮，如果管理员已经完成工作，请务必退出登录。同时，管理界面设置了会话时间的限制，如果管理员在一段时间内无操作，系统将自动 关闭会话过程，并提示管理员需要重新登录系统。

4 功能详解

4.1 系统状态

CACTER 邮件安全云网关系统在网关首页会显示当日邮件接收情况概览，包括今日接收邮件总量，正常邮件、垃圾邮件、恶意邮件的数量，各类邮件占比以及每个时段各类邮件的接收情况统计。

CACTER 邮件安全云网关系统在网关首页会显示当日的网关运行信息，包括今日邮件流量情况、今日恶意垃圾邮件趋势、恶意垃圾邮件主题 TOP10 信息、恶意垃圾邮件外部发信人 TOP10 信息。



- **接收邮件流量情况**

显示网关当日邮件接收情况概览，包括各类邮件的数量，各类邮件占比和。

- **今日恶意垃圾邮件趋势**

显示网关当天每个时段各类邮件的接收统计。

- **恶意垃圾邮件主题TOP10**

显示网关接收的恶意垃圾邮件主题 top 信息，包括排名（展示前十名）、邮件主题、数量，方便管理员快速知晓当日接收的恶意邮件主要主题信息。

- **恶意垃圾邮件外部发信人TOP10**

显示网关接收的恶意垃圾邮件外部发信人 top 信息，包括排名（展示前十名）、外部发信人、数量，方便管理员快速知晓当日接收的恶意邮件主要外部发信人信息。

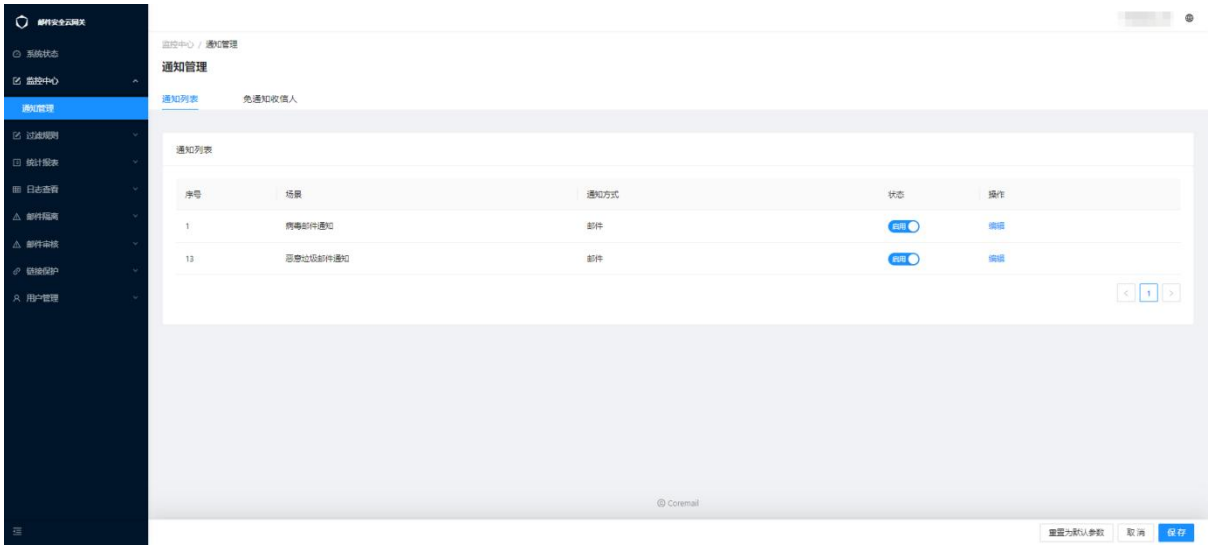
4.2监控中心

4.2.1 通知管理

云网关默认使用 emailgateway@cacter.com 作为发信邮箱。

- **通知列表**

管理员可以对病毒邮件通知、恶意垃圾邮件通知两大场景进行统一监控管理，自行设定该通知场景启用或者禁用。



1）病毒邮件通知

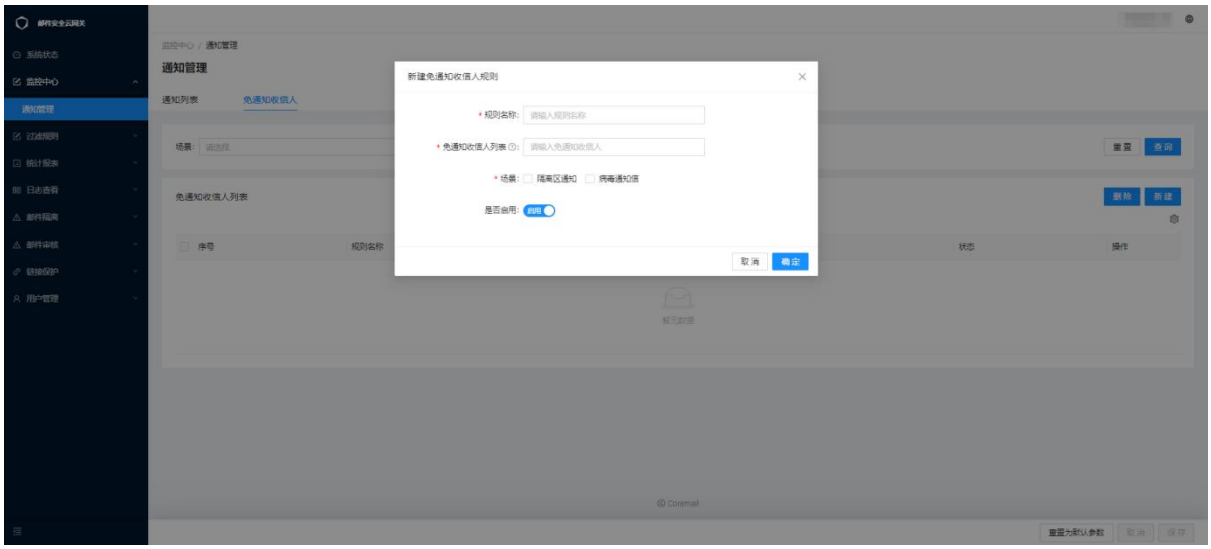
管理员点击【编辑】按钮，进入病毒邮件通知编辑弹窗，可选择是否开启该功能，以及自定义配置通知信是否带病毒附件。

2）恶意垃圾邮件通知告警

管理员点击【编辑】按钮，进入恶意垃圾邮件通知告警编辑弹窗，可选择是否开启该功能，并且自定义恶意垃圾邮件通知告警的邮箱。启用后，恶意垃圾邮件由于白名单机制而绕过网关检查，将通知管理员。

- 免通知收信人

可针对单个或者多个收信人添加【免通知收信人规则】，可以免除通知的通知信类型有病毒通知信、隔离区通知信。



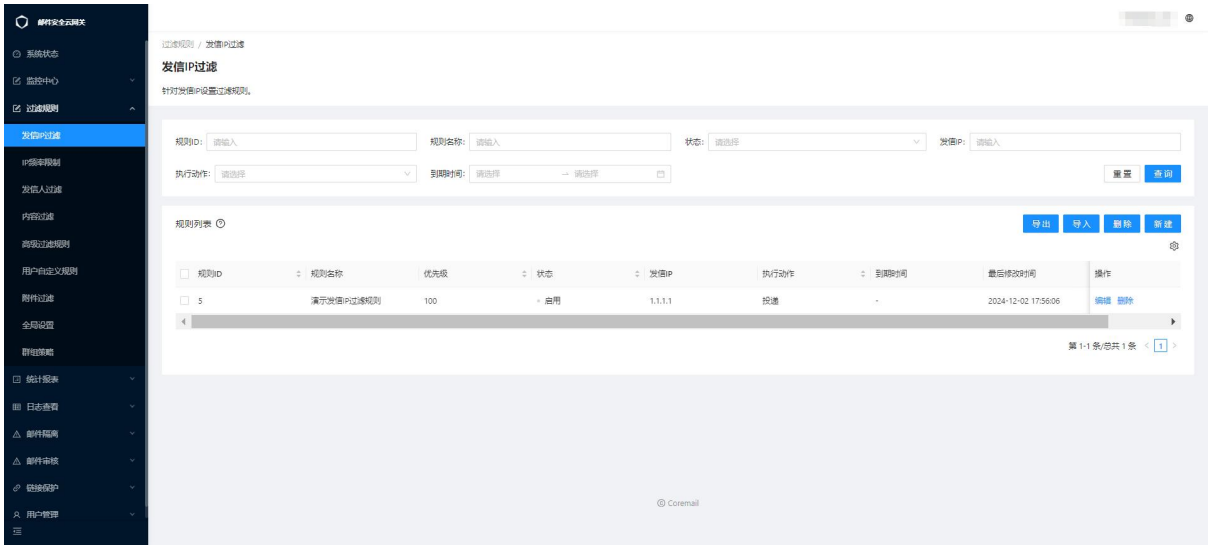
4.3 过滤规则

4.3.1 发信 IP 过滤（路径：过滤规则-发信 IP 过滤）

发信 IP 过滤是基于邮件发信人的 IP 地址设定的邮件判定规则。管理员可以将已知的垃圾邮件发送者的 IP 地址作为匹配条件，对符合条件的邮件设定执行动作，从而实现对来自该 IP 的电子邮件进行处理。

控件按钮说明：

- 【重置】按钮：管理员在发信IP过滤页面上方模糊搜索栏输入查询关键字等筛选条件，点击页面“重置”按钮，清空模糊搜索栏已输入的关键字和筛选条件。
- 【查询】按钮：管理员在发信IP过滤页面上方模糊搜索栏输入查询关键字等筛选条件，点击页面“查询”按钮，查询已有发信人IP过滤规则。
- 【导入】按钮：管理员点击发信IP过滤页面的“导入”按钮，弹出导入规则弹出，点击上传文件即可本地上传，点击模板下载即可下载模板到本地编辑后上传。
- 【导出】按钮：管理员点击发信IP过滤页面的“导出”按钮，可导出所有发信人规则到本地。
- 【新建】按钮：管理员点击发信IP过滤页面“新建”按钮进入新建发信IP过滤规则弹窗，可对规则名称、优先级、IP地址（IP/IP组）、执行动作、到期时间等可编辑属性进行编辑。
- 【删除】文本按钮：管理员点击发信IP过滤规则列表的“删除”按钮，可删除该发件IP规则。
- 【编辑】文本按钮：管理员点击发信IP过滤规则列表的“编辑”按钮，可编辑发件IP规则，并设置是否启用规则。

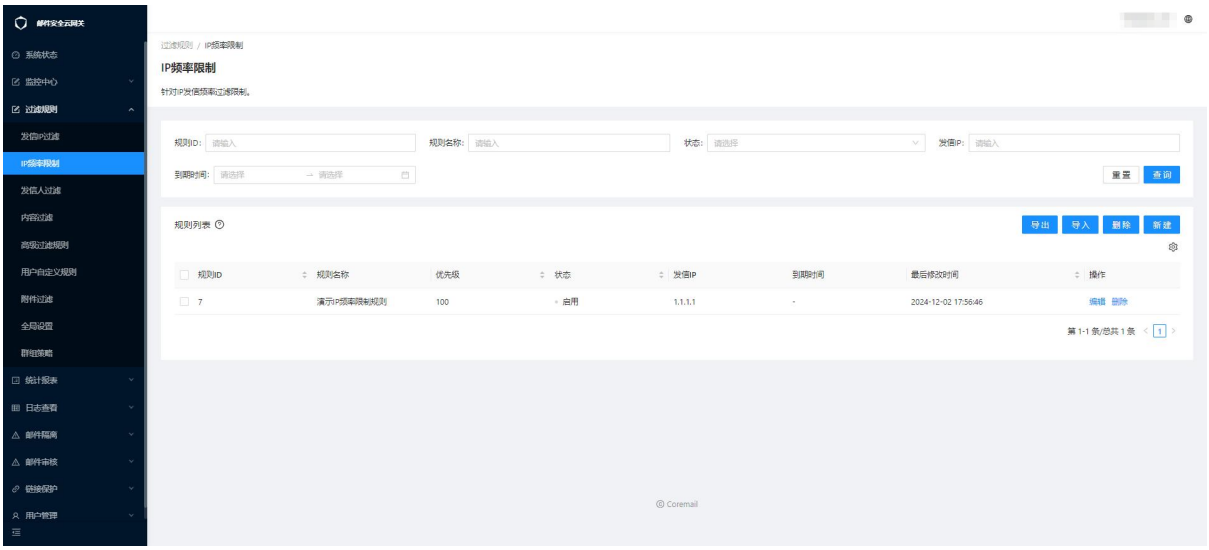


4.3.2 IP 频率限制（路径：过滤规则-IP 频率限制)

IP 频率限制是基于邮件发信人的 IP 地址设定的邮件过滤规则。管理员可以将已知的垃圾 邮件发送者的 IP 地址作为匹配条件，对符合条件的 IP 地址设定邮件规则，执行 IP 连接频率 控制，从而实现对来自这 IP 的电子邮件进行处理。

控件按钮说明：

- 【新建】按钮：点击按钮弹出新建频率限制规则弹窗，可以对规则名称、优先级、发信IP、同时连接数上限、每15分钟连接数上限、每日连接数上限、IP每小时SMTP认证失败次数上线、每个链接SMTP认证次数上线、到期时间等可编辑属性进行编辑保存。
- 【查询】按钮：在IP频率限制页面顶部模糊搜索栏里选择编辑筛选条件，点击查询按钮即可在下方列表展示相关信息搜索结果。
- 【重置】按钮：点击此按钮即可对模糊搜索栏已选择筛选条件清空。
- 【编辑】文本按钮：点击规则列表编辑文本按钮可以对列表内已编辑的规则做二次修改。
- 【删除】文本按钮：点击规则列表删除文本按钮可以对列表已录入规则做删除操作。



4.3.3 发信人过滤（路径：过滤规则-发信人过滤）

发信人过滤是基于邮件收发信人的邮箱地址、所使用的 IP 地址设定的邮件判定规则。 例如管理员可以将已知的垃圾邮件发送者的邮箱地址、或者将某个 IP 地址以及对应使用的某个邮箱地址进行组合，设定邮件规则，对此一类发信人执行邮件发垃圾策略，从而实现对 来自这 些邮箱地址的电子邮件进行处理。

控件按钮说明：

【新建】：管理员点击发信人规则页面“新建”按钮，创建新的发件人规则。

【查询】：管理员输入查询关键字等筛选条件，点击发件人规则页面“查询”按钮，查询已有发信人规则。

【删除】：管理员点击发信人规则的“删除”按钮，可删除该发件人规则。

【编辑】：管理员点击发信人规则的“编辑”按钮，可编辑发件人规则，并设置是否启用规则。

【导入】：管理员点击发信人规则的“导入”按钮，可按照规范上传添加发信人规则。

【导出】：管理员点击发信人规则的“导出”按钮，可导出所有发信人规则。

新建发信人过滤规则

点击“新建规则”按钮，在弹出框输入发信人规则名称、匹配条件及具体设置，点击保存即可。

发信人过滤规则查询

发信人规则查询提供：规则 ID、规则名称、状态、发信人、发信人 IP、执行动作，管理员可根据具体情况，灵活组合信息以查找发信人过滤规则。

发信人规则列表

页面默认显示系统所有发信人过滤规则，并列出规则包含的所有信息，方便用户快速查找。

1. 管理员查询规则时，可通过对各条件进行组合查询。

2. 规则列表支持排序，管理员可通过点击“规则 ID”、“优先级”、“状态”、“执行动作”、“最后修改时间”对规则列表进行排列。

4.3.4 内容过滤（路径：过滤规则-内容过滤）

内容过滤是基于邮件信头、主题、正文、附件名、附件内容所出现的文字所设定的邮件过滤规则。

例如，管理员可以根据垃圾邮件出现在信头、正文、附件名、附件内容上的常用字符，设定反垃圾邮件关键字规则，从而把邮件信头、正文、附件名含有关键字的电子邮件判别为垃圾邮件。

控件按钮说明：

- 【重置】按钮：管理员在内容过滤页面上方模糊搜索栏输入查询关键字等筛选条件，点击页面“重置”按钮，清空模糊搜索栏已输入的关键字和筛选条件。
- 【查询】按钮：管理员在内容过滤页面上方模糊搜索栏输入查询关键字等筛选条件，点击页面“查询”按钮，查询已有内容过滤规则。

- 【新建】按钮：管理员点击内容过滤页面“新建”按钮进入新建内容过滤规则弹窗，可对规则名称、优先级、内容（内容文本或正则表达式）/内容组、规则作用于邮件主体不同部分、执行动作、到期时间等进行编辑保存。
- 【删除】文本按钮：管理员点击内容过滤规则列表的“删除”按钮，可删除该内容过滤规则。
- 【编辑】文本按钮：管理员点击内容过滤规则列表的“编辑”按钮，可编辑内容规则，并设置是否启用规则。

正则表达式：

在搜索中使用正则表达式时，特定的规则将控制哪些字符组合将执行特定的匹配操作。每种正则表达式（或正则表达式的组合）都称为“语法”。可以在内容规则编辑弹窗中选中正则表达式以精确匹配要搜索的目标。

4.3.5 高级过滤规则（路径：过滤规则-高级过滤规则）

高级过滤规则不仅可以设置内容过滤包含的字段，还能对与发信IP、发信人地址、收信人地址进行结合，设置更为精确的内容过滤规则。

例如：

管理员可以根据垃圾邮件的来源IP，结合出现在信头、正文、附件名上的常用字符，设定针对这个IP发送的垃圾邮件进行拦截操作。

控件按钮说明：

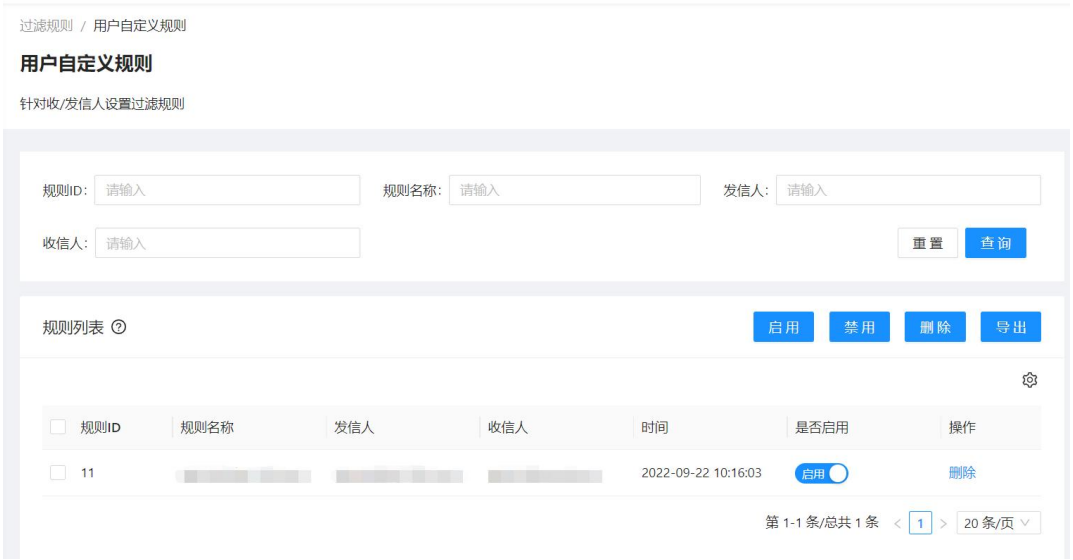
- 【重置】按钮：管理员在高级内容过滤页面上方模糊搜索栏输入查询关键字等筛选条件，点击页面“重置”按钮，清空模糊搜索栏已输入的关键字和筛选条件。
- 【查询】按钮：管理员在高级内容过滤页面上方模糊搜索栏输入查询关键字等筛选条件，点击页面“查询”按钮，查询已有高级内容过滤规则。

- 【新建】按钮：管理员点击高级内容过滤页面“新建”按钮进入新建高级内容过滤规则弹窗，可对规则名称、优先级、触发执行动作、作用邮件方和IP地址、执行动作。
- 【新建】按钮：管理员点击高级内容过滤页面“新建”按钮进入新建高级内容过滤规则弹窗，可对规则名称、优先级、触发执行动作、管控邮件范围、作用邮件方和IP地址、执行动作、到期时间等进行编辑保存。
- 【删除】文本按钮：管理员点击内容过滤规则列表的“删除”按钮，可删除该高级过滤规则。
- 【编辑】文本按钮：管理员点击内容过滤规则列表的“编辑”按钮，可编辑高级过滤规则，并设置是否启用规则。

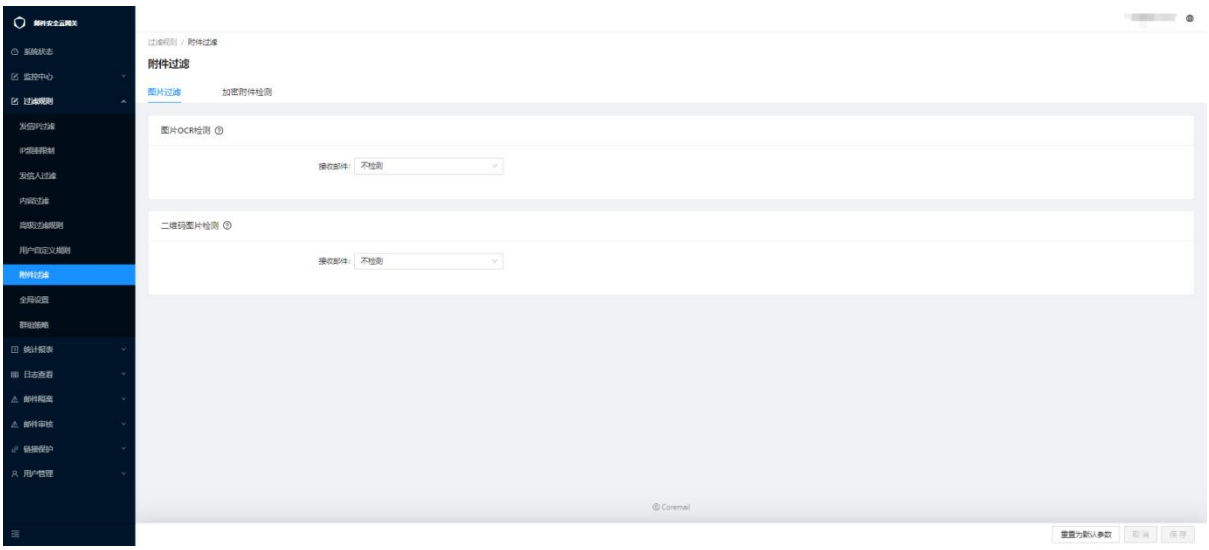
4.3.6 用户自定义规则（路径：过滤规则-用户自定义规则）

【白名单】操作按钮：用户收到隔离区通知信后，点击【白名单】，可自动在网关生成一条户自定义规则。如下图4-2所示，点击【白名单】，在网关生成一条自定义规则，如图4-3

管理员可对该条自定义规则设置，进行【启用】/【禁用】/【删除】/【导出】操作。



4.3.7 附件过滤（路径：过滤规则-附件过滤）



CACTER邮件安全云网关新增附件过滤模块，支持对图片过滤功能进行配置（包括图片OCR检测、二维码图片检测）、支持加密附件检测功能配置。

图片OCR检测：管理员可选择【不检测】或者【OCR深度识别检测】，并可配置单个附件OCR识别检测数量上限。

二维码图片检测：管理员可选择【不检测】/【审核】/【阻断】/【丢弃】/【二维码图片深度检测】，并可配置单个附件二维码图片深度检测数量上限。

加密附件检测：管理员可选择【不检测】/【隔离/审核】/【阻断】/【加密附件深度检测】，并可针对加密附件解密失败的邮件配置处理操作，包括【进行下一步检测】/【隔离/审核】/【阻断】/【丢弃】。

4.3.8 全局设置（路径：过滤规则-全局设置）

管理员可以对网关过滤能力进行全局调整，包括恶意攻击防御、仿冒邮件检测、接收邮件控制以及高级设置。

恶意攻击防御

单连接控制：包括每个连接命令次数上限、每个连接命令错误次数上限以及每个连接SMTP认证失败次数上限。

仿冒邮件检测

管理员可根据仿冒邮件的发信行为特征，如是否允许Mail From命令的内容为空、是否允许Mail From使用不存在的用户或者非法用户等，动态调整全局配置。管理员也可选择是否开启全局SPF检查、DKIM检查、DMARC检查。

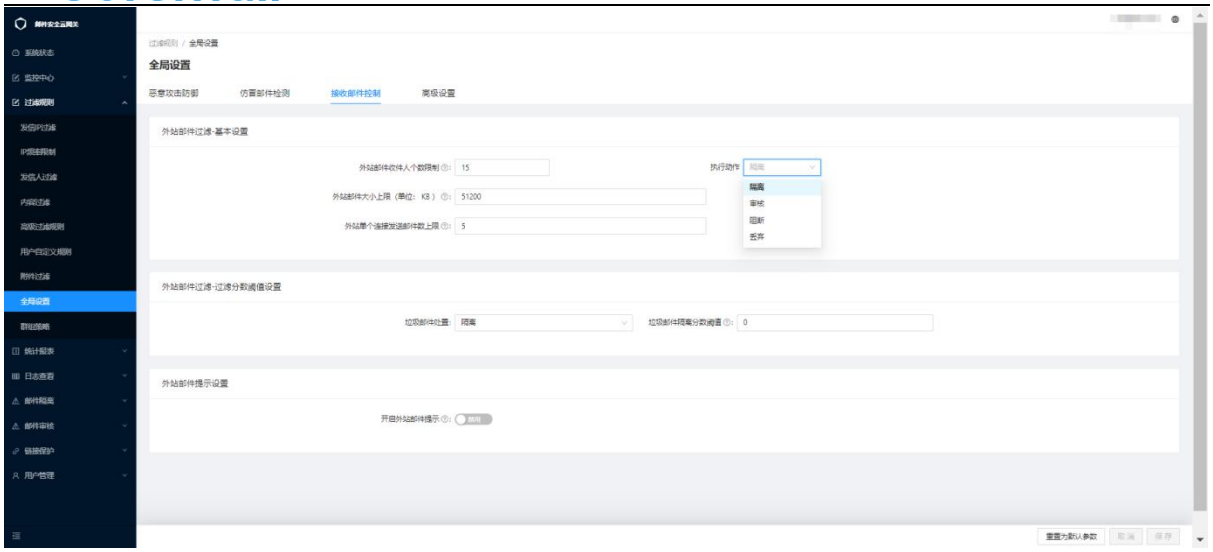
若要启用DMARC检查，需先开启DKIM认证。

接收邮件控制

1）基本设置和附件设置

管理员可根据外部邮件的发信行为特征，调整全局过滤参数。

发信行为特征包括外站邮件收件人个数限制、外站邮件大小上限、外站单个连接发送邮件数上限、外站邮件附件个数上限。其中外站邮件收信人除了可以配置限制收件人个数外，还可以配置执行动作，如下图所示，若执行动作若选择隔离，当外站邮件收信人个数超过配置值的时候，该邮件将进入隔离区；且管理员可以在隔离区决定该邮件可以投递给哪些收信人。



2）过滤分数阈值设置

网关支持针对垃圾邮件隔离分数阈值，动态调整适合客户邮件使用情况，分数调整区间为[0,1]。当垃圾邮件分数高于设定的阈值时，邮件将被隔离。网关同时也支持将部分垃圾邮件打上【垃圾邮件】的标签投递至邮件系统的垃圾邮件文件夹，管理员可按需配置是否开启该功能，配置文档见附件一。

3）外站邮件提示设置

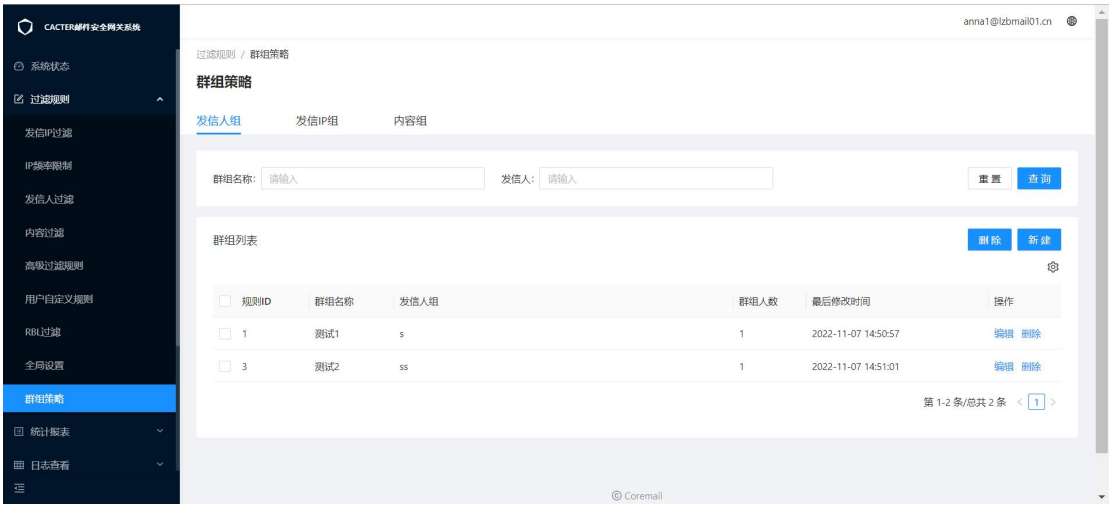
网关支持对外站邮件进行提示，管理员可选择是否开启。开启后，若用户收到来自外站的邮件，将在邮件正文前进行提醒。

高级设置

- 可设置是否允许IP挂起操作、相似邮件数量阈值。
- 支持开启和关闭URL链接保护功能，可按需开启未知URL访问提醒。

4.3.9 群组策略（路径：过滤规则-群组策略）

管理员可以创建不同的发信人组、发信IP组和内容组，并且针对该组发信人、发信IP、内容设置相应的过滤规则。



控件按钮说明：

- 【重置】按钮：管理员在群组策略页面上方模糊搜索栏输入群组名称等筛选条件，点击页面“重置”按钮，清空模糊搜索栏已输入的群组名称等筛选条件。
- 【查询】按钮：管理员在群组策略页面上方模糊搜索栏输入群组名称等筛选条件，点击页面“查询”按钮，查询已有群组。
- 【编辑】文本按钮：管理员点击群组列表的“编辑”按钮，可对群组进行修改。
- 【删除】文本按钮：管理员点击群组列表的“删除”按钮，可删除该条群组。
- 【新建】按钮：管理员点击群组策略页面“新建”按钮，进入新建群组弹窗，建立相应群组

- **发信人组**

管理员点击发信人组页面“新建”按钮，进入新建群组弹窗，可建立发信人群组。

发信人组设置成功后，可在过滤规则-发信人过滤中，引用设置的发信人组新建发信人过滤规则。

- **发信IP组**

管理员点击发信IP组页面“新建”按钮，进入新建群组弹窗，可建立发信IP群组。

发信IP组设置成功后，可在过滤规则-发信IP过滤中，引用设置的发信IP组新建发信IP过滤规则。

- **内容组**

管理员点击内容组页面“新建”按钮，进入新建群组弹窗，可建立内容群组。

内容组设置成功后，可在过滤规则-内容过滤中，引用设置的内容组新建内容过滤规则。

4.4 统计报表

CACTER 邮件安全云网关系统提供包括邮件过滤统计、邮件类型统计、TOP统计三大功能，分别针对网关处理邮件的执行动作、邮件的具体类型以及发信 IP 的链接情况进行统计。通过这些统计数据，管理员可以了解网关的运行情况。

4.4.1 邮件过滤统计（路径：统计报表-邮件过滤统计）

根据网关对邮件的执行动作，可分为投递、隔离、审核、阻断、丢弃、灰名单、无效链接。邮件过滤统计将记录每日邮件接收/外发/域内的过滤情况，以柱状图和数据表形式展示，管理员可调整统计时间和单位，进行查询。

字段说明：

- 投递：邮件经过网关检测过滤，或命中管理员自定义的过滤规则，投递到邮件系统；管理员自定义的投递过滤规则，主题添加自定义标签，则为标记投递。
- 隔离：接收邮件被网关检测为垃圾邮件并达到隔离阈值，或命中管理员自定义的过滤规则，存放到网关的隔离区。

- 审核：外发垃圾邮件被网关检测为垃圾邮件并达到审核阈值，或命中管理员自定义的过滤规则，存放到网关的审核队列中。
- 阻断：邮件不满足网关的全局设置规则，或为病毒邮件，或命中管理员自定义的过滤规则，拒收邮件即为阻断，“阻断”发信人会收到退信通知。
- 丢弃：邮件命中管理员自定义的过滤规则，或命中RBL过滤且动作为丢弃，则网关将收下邮件后再丢弃，“丢弃”发信人不会收到退信通知。
- 灰名单：邮件命中RBL过滤且动作为灰名单，则执行灰名单动作；灰名单即：同一封邮件第一次检测被拒绝，第二次会通过。
- 无效连接：网关实际未接收到邮件的无效连接。

按钮控件说明：

- 【下载】按钮：点击即可自动转为PDF版文件且下载至本地。

按钮控件说明：

【下载】按钮：点击即可自动转为PDF版文件且下载至本地。

4.4.2 邮件类型统计（路径：统计报表-邮件类型统计）

根据邮件的具体类型，CACTER邮件安全网关系统对邮件分为正常邮件、普通垃圾邮件、可疑垃圾邮件、高风险垃圾邮件、恶意邮件—钓鱼邮件、恶意邮件—病毒邮件、无效邮件。邮件过滤统计将记录每日接收的各类邮件情况，以柱状图和数据表形式展示，管理员可调整统计时间和单位，进行查询。

邮件分类：

1. 正常邮件：邮件经过网关检测过滤，或命中管理员自定义的过滤规则，投递到邮件系统的邮件。
2. 普通垃圾邮件：邮件被网关检测为普通垃圾邮件，或命中管理员自定义的过滤规则，存放到网关隔离区或者阻断的邮件。
3. 可疑垃圾邮件：邮件有加密附件、二维码疑似威胁，相关的邮件会被定义为可疑垃圾邮件。
4. 高风险垃圾邮件：邮件被网关检测为SPF、DKIM、DMARC不通过，相关的邮件会被定义为高风险垃圾邮件。
5. 恶意邮件—钓鱼邮件：邮件被网关检测为钓鱼邮件，存放到网关的隔离区或者阻断的邮件。
6. 恶意邮件—病毒邮件：邮件被网关检测为病毒邮件，阻断的邮件。
7. 无效邮件：邮件连接中断，实际未被网关接收的邮件。

4.4.3 TOP 统计（路径：统计报表-TOP 统计）

CACTER邮件安全网关系统支持针对IP连接进行TOP统计。管理员可自定义TOP统计数和统计日期范围，默认显示当天10条统计记录。

- IP连接统计

CACTER邮件安全网关系统对每个IP的连接情况进行记录统计，分为IP连接总数、IP连接成功次数和IP连接失败次数。管理员可以按需进行升降序排列，查询特定日期的IP连接统计情况。点击某一IP可跳转邮件投递日志页面，查看该IP的邮件投递详情信息。

按钮控件说明：

- 【重置】按钮：清空已选择或填入的筛选条件。
- 【查询】按钮;根据已选择或填入的筛选条件筛选出符合条件的列表信息。
- 【导出】按钮：支持将查询结果以.csv格式下载保存到本地，下载导出量按照顶部设置的显示数量，下载当页展示的列表信息。

4.5 日志查看

1.CACTER邮件安全网关系统向管理员提供邮件投递日志、恶意邮件日志、链接保护日志、系统通知信日志和管理员操作日志的查询功能。

2.通过各页面上方模糊搜索栏里的筛选条件即可筛选已存入日志记录，可对日志进行查看详情及下载操作。（管理员日志只有查看权限）

4.5.1 邮件投递日志（路径：日志查看-邮件投递日志）

通过邮件投递日志，管理员可以查看了解邮件的投递情况。邮件日志列表显示收发类型、发信IP、发信人、收信人、主题、URL、附件 MD5、邮件评分、执行动作、原因、邮件类型、投递状态。管理员可以自定义搜索条件，定位具体邮件的相关日志。其中，

1.收发类型：显示邮件的收发方向。

2.邮件评分：显示反垃圾引擎对邮件内容进行的评分结果，分数越高，垃圾邮件可能性约高。

3.执行动作：显示邮件被网关执行的动作，包括投递、标记投递、隔离、阻断、丢弃、审核、灰名单。

4.原因：显示邮件被执行动作的具体原因。

5.投递状态：显示邮件投递的状态信息，包括投递中、投递成功、投递失败、部分失败。

邮件投递日志支持导出，管理员可点击对应日志条目进行查看详情，并下载到本地。

4.5.2 恶意邮件日志（路径：日志查看-恶意邮件日志）

网关会将反垃圾引擎检测出的恶意邮件日志进行单独展示，管理员可快速知晓域内威胁情况，快速做出响应处理。恶意邮件包括钓鱼邮件、病毒邮件。

恶意邮件日志支持搜索、查看和下载，操作方式与邮件投递日志相似。

4.5.3 链接保护日志（路径：日志查看-链接保护日志）

当管理员开启链接保护功能后，会记录每一封保护的邮件的相关日志信息。管理员可以通过URL、发信人、收信人、URL 类型进行查询，了解未知链接的具体访问情况。

名词定义如下：

- 原始 URL：原始邮件中的 URL 链接。
- 保护后 URL：原始链接被保护后生成的 URL 链接。
- 对于 URL 类型，网关将其分为未知 URL、安全 URL、威胁 URL、未访问 URL：
- 未知 URL：用户访问后，检测结果为未知的 URL 链接。
- 安全 URL：用户访问后，检测结果为安全的 URL 链接。
- 威胁 URL：用户访问后，检测结果为威胁的 URL 链接。
- 未访问 URL：用户未访问的 URL 链接。

例如，管理可以在搜索条件的 URL 中，输入某个恶意链接，查询包含该恶意链接的所有邮件，定位已访问用户，进行针对性通知管理。

4.5.4 系统通知信日志（路径：日志查看-系统通知信日志）

网关会对系统发出的各类通知邮件进行单独展示，管理员可以快速查看和了解系统通知邮件的投递情况。日志列表显示发信人、收信人、主题、邮件类型、投递状态。管理员可以自定义搜索条件，定位具体邮件的相关日志。

系统通知信日志支持导出，管理员可点击对应日志条目进行查看详情，并下载到本地。

4.5.5 管理员操作日志（路径：日志查看-管理员操作日志）

在管理员操作日志功能，管理员可查看操作人员、操作时间、登录 IP、操作行为、操作结果等信息。包括管理员对安全策略(如邮件过滤策略等)进行更改的操作、授权管理员的登录和退出、对用户角色进行增删查改操作等。

4.6 邮件隔离

4.6.1 邮件隔离区（路径：邮件隔离-邮件隔离区）

CACTER邮件安全网关系统会将已识别的垃圾邮件隔离在邮件隔离区，保证投递到邮件系统中邮件的安全性。管理员也可以通过设置过滤规则，将符合已知垃圾邮件特征的可疑邮件投递到隔离区，避免对域内邮件安全造成威胁。

- **隔离邮件查询**

管理页面默认显示所有隔离邮件，并显示邮件的主要信息，包括发信IP、发信人、收信人、主题、URL、邮件MD5、邮件评分、原因、邮件类型、投递状态、状态等。管理员可根据需求，搜索查看具体的隔离邮件信息。其中，

邮件评分：显示反垃圾引擎对邮件内容进行的评分结果。

原因：显示邮件被隔离的具体原因。

状态：显示邮件目前的状态，包括隔离、已投递、已取回、已删除、已过期。

投递状态：显示邮件目前的投递状态，包括投递中、投递成功、投递失败、部分失败。

- **隔离邮件操作**

网关对进入到隔离区的可疑垃圾邮件，提供包括投递、添加白名单、查看、下载、删除在内的管理操作，协助管理员管理隔离邮件。其中，

投递：将邮件重新投递到对应的收件人邮箱。

白名单：可一键将发信人添加白名单。

查看：显示网关对邮件的分析日志、邮件的具体内容。

下载日志：可下载邮件日志到本地。

下载邮件：可下载邮件原件到本地。

删除：删除指定隔离邮件。

批量功能：可以选中多个邮件，进行批量投递，批量白名单和批量删除操作。

4.6.2 隔离区设置（路径：邮件隔离-隔离群设置）

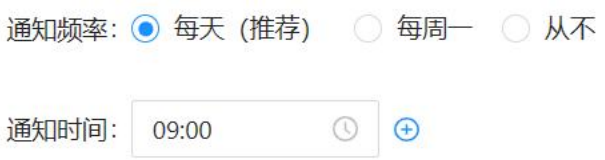
管理员可设置隔离区邮件的保存周期和通知设置。

- **隔离邮件基础设置**

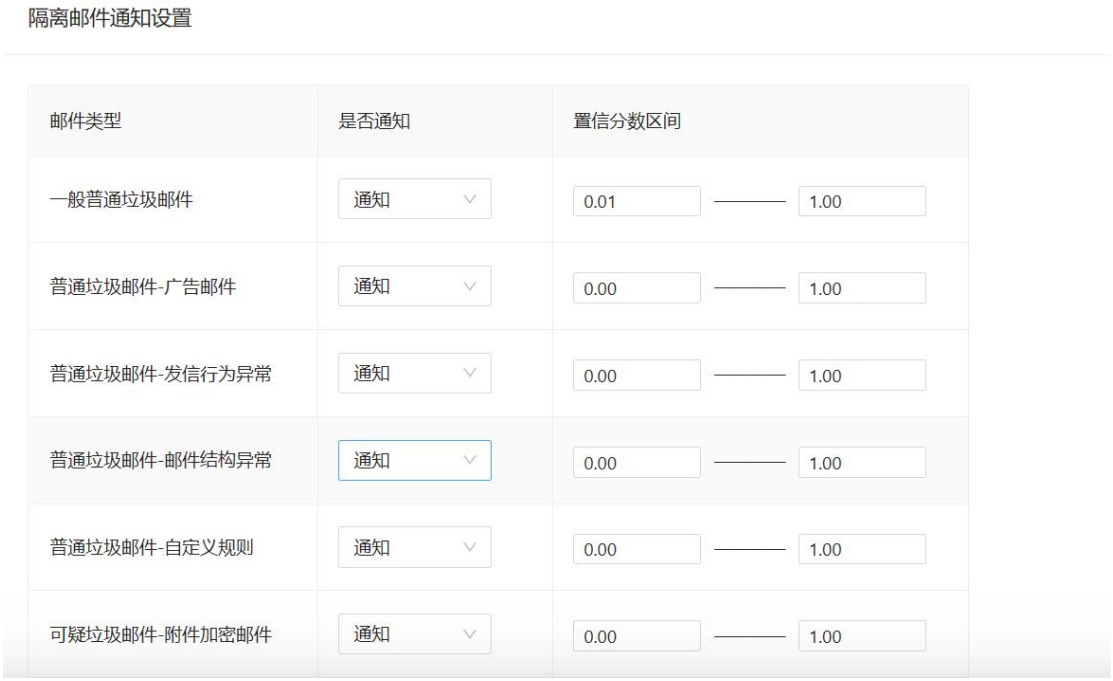
隔离区邮件网关默认保存30天，功能优化中，暂不支持修改设置。

- **隔离邮件通知设置**

网关支持调整隔离区邮件通知频率，默认为每天通知，可调整为每周一或者从不通知。通知时间默认为09:00，也可以添加不同通知时间点。



网关也支持根据不同邮件类型，自定义是否发送隔离邮件通知，以及自定义隔离区通知邮件的置信分数区间。网关只会对邮件评分在设置的分数区间内的邮件，发送隔离区通知邮件信；在分数区间外的隔离邮件不通知用户。



- **隔离邮件用户权限设置**

管理员可按需启用隔离邮件通知信的取回、白名单和黑名单功能，并且灵活配置其有效时间。启用后，用户收到的隔离邮件通知信将会显示相关功能按钮，用户可针对隔离邮件通知信，在有效期内进行取回、添加个人白名单和个人黑名单的操作。超出设定的有效期，用户将无法进行取回、添加个人白名单和个人黑名单操作。

4.7 邮件审核

4.7.1 邮件审核队列（路径：邮件审核-邮件审核队列）

CACTER邮件安全网关系统会将超过设定的审核阈值外发垃圾邮件，存放到邮件审核队列，保证投递到外发邮件的合法性。管理员也可以通过设置过滤规则，将需要审核的邮件存放到审核队列。

- **邮件审核队列查询**

页面默认显示所有待审核邮件，并显示邮件的主要信息，包括收发类型、主题、发信IP、发信人、收信人、邮件评分、原因等。管理员可根据需求，搜索查看具体的待审核邮件信息。其中，

邮件评分：显示反垃圾引擎对邮件内容进行的评分结果。

原因：显示邮件列入审核队列的具体原因。

- **审核邮件操作**

网关对进入到审核队列的邮件，提供包括投递、添加白名单、查看、下载、删除在内的管理操作。其中，

名词定义：

投递：将邮件重新投递到对应的收件人邮箱。

白名单：可一键将发信人添加白名单。

查看：显示网关对邮件的分析日志、邮件的具体内容。

下载：可下载邮件原件到本地。

删除：删除指定的待审核邮件。

批量功能：可以选中多个邮件，进行批量投递，批量白名单和批量删除操作。

4.7.2 邮件审核日志（路径：邮件审核-邮件审核日志）

通过邮件审核日志，管理员可以查看了解历史邮件的审核情况。邮件日志列表显示邮件的收发时间、发信IP、发信人、收信人、主题、邮件评分、原因、审核结果、审核管理员以及操作时间。管理员通过上方模糊搜索栏中筛选条件，定位具体邮件的相关日志。

4.7.3 邮件审核设置（路径：邮件审核-邮件审核设置）

管理员可设置邮件的审核操作和通知设置。

- **邮件审核基础设置**

邮件审核周期默认为24小时，功能优化中，暂不支持修改设置。

当邮件超过审核周期时，邮件默认执行投递。管理员可设置关闭，即邮件超出审核周期时，直接丢弃。

- **邮件审核通知设置**

邮件审核结果默认通知到发信人，管理员也可设置为关闭，即不发送通知信息。

管理员可根据管理需求，设置多个审核通知接收邮箱，当存在待审核邮件时，系统会按照设定的通知频率发送通知邮件。管理员再登录网关系统进行邮件审核操作。

审核邮件通知频率，默认为每30分钟通知一次。通知信发送时间区间默认为00:00~23：59，均可按需调整。

4.8 链接保护

对于首次链接检测结果未知的链接，CACTER 邮件安全云网关系统推出了链接保护功能，作为第二道安全检测门槛。当用户查看已被链接保护的 URL 时，会向云端发起链接安全性查询，若链接返回为恶意链接/未知链接，页面将给予不同的提示，保证用户链接访问安全。连接邮件通过该功能，管理员可以快速追踪收到钓鱼邮件的用户操作情况，包括哪些用户访问的链接为钓鱼链接、域内点击量最高的钓鱼链接情况等等。

4.8.1 链接保护统计（路径：链接保护-链接保护统计）

页面展示链接保护功能的运行情况，包括今日点击恶意链接用户数、今日恶意链接点击次数、今日邮件保护情况、今日链接保护情况、邮件保护数量统计、链接保护数量统计、链接点击次数排行、点击链接次数最多的用户排行。

- **今日点击恶意链接用户数**

  显示今日点击恶意链接用户数，并根据上次出现点击恶意用户数量情况，进行对比提示。

- **今日恶意链接点击次数**

  显示今日恶意链接点击次数，并根据上次出现恶意链接点击次数情况，进行对比提示。

- **今日邮件保护情况**

  显示今日邮件保护情况，包括检测隔离的钓鱼邮件数和进行链接保护的邮件数，并按照邮件占比进行统计。

- **今日链接保护情况**

  显示今日链接保护总数，并按照链接类型进行占比统计，包括：安全链接、恶意链接、未知链接、未点击链接。

- **邮件保护数量统计**

  可选定时间范围统计邮件保护数量，了解链接保护功能运行情况。

- **链接保护数量统计**

  可选定时间范围统计链接保护数量，了解链接保护功能运行情况。

- **链接点击次数排行**

  默认显示当日链接点击次数的域名排行，可根据需求选择近 7 天，近 30 日进行统计。

- **点击链接次数最多的用户排行**

  默认显示当日点击链接次数最多的用户排行，可根据需求选择近 7 天，近 30 日进行统计。

4.8.2 链接保护白名单（路径：链接保护-链接保护白名单）

管理员可以根据需求，将可信的邮件来源添加至白名单。包括发信人白名单、收信人白名单、URL 白名单。

- **发信人白名单**

  将可信发信人加入白名单，链接保护功能对该来源邮件不启用.

- **收信人白名单**

  将指定发信人加入白名单，链接保护功能对发往该收信人的邮件不启用。

- **URL 白名单**

  将可信 URL 加入白名单，链接保护功能对该 URL 链接不启用。

  URL白名单支持匹配方式：

  1.支持域名填写，域名填写将会模糊匹配URL

  2.URL填写，将完全匹配URL

  3.支持子域名匹配

  4. 匹配指定的单个IPv4地址：x.x.x.x

  5. 匹配指定的IPv4网段：x.x.x.x-x.x.x.x

  6. 匹配指定的IPv4子网：x.x.x.x/x

  7. 匹配多个IPv4：x.x.x.x;x.x.x.x

  8. 匹配除这些IP外的地址：!x.x.x.x;x.x.x.x

4.9 用户管理

用户管理模块提供帐号安全、登录设置、管理员设置和角色权限功能，协助超级管理员对网关用户进行管理。

4.9.1 帐号安全（路径：用户管理-账号安全）

账号信息

在此模块可以查看管理员个人账号信息，包括手机号，邮箱账号等；并可以在此绑定/修改手机号，邮箱账号信息。

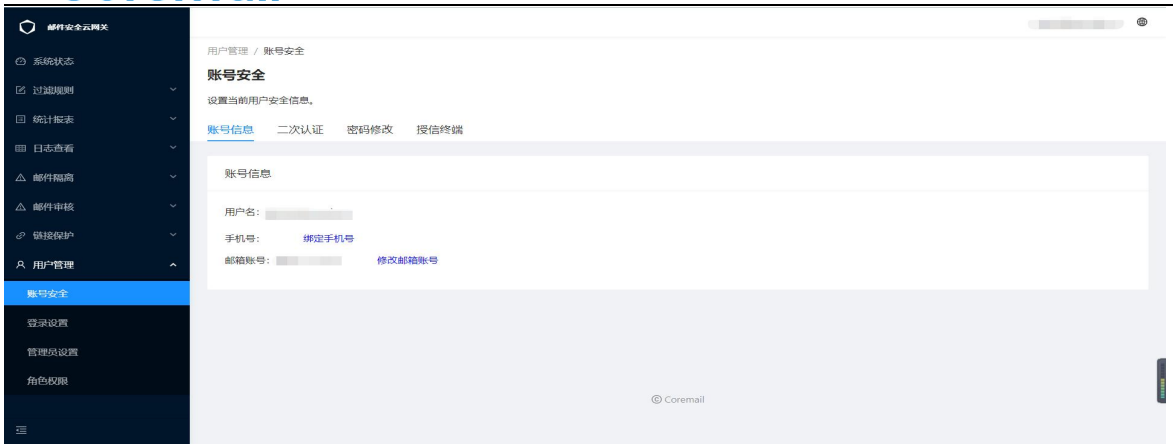


图 4-4

二次认证

管理员可根据自身登录需求，开启二次认证。二次认证支持短信认证和邮箱认证两种认证方式。

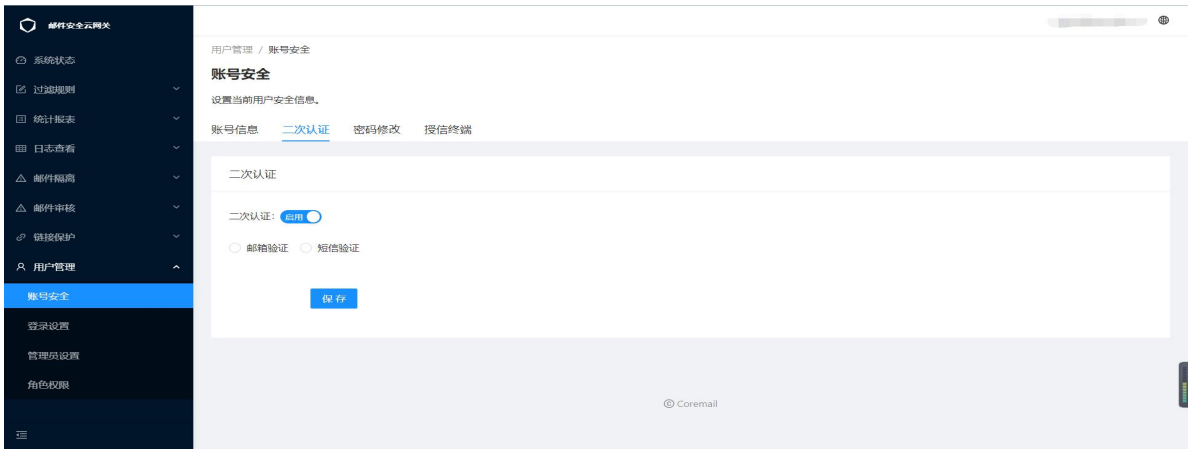


图 4-5

密码修改

管理员可以修改本帐号的登录密码，确保帐号安全。

授信终端

管理员登录时候可以添加授信终端；也可以在此处取消可信任。

4.9.2 登录设置（路径：用户管理-登录设置）

超级管理员可以针对管理员的登录请求进行检查配置，包括重复当日密码错误次数上限、 会话超时时间。超级管理员还可以限制所有管理员登录 IP 范围，来提供网关访问的安全性。

4.9.3 管理员设置（路径：用户管理-管理员设置）

超级管理员可以对网关的其他管理员进行查看、新增、编辑、删除操作，并可重置其他管理员的登录密码、角色类型分配。

全域二次认证

超级管理员（角色），可以启用/禁用，全域二次认证。

启用：全域管理员用户登录场景均需进行二次认证。

禁用：不对全域管理员登录场景二次认证做强制性要求，管理员可根据自身登录安全需求，自行在【账号安全】处开启/选择二次认证方式。

新建管理员

1）点击【新建管理员】按钮：可配置相应的角色名称，赋予管理员对应的功能权限，可限制管理员账号到期时间、备注相关信息，以及通过角色列表查看已有的历史角色信息。

2）启用/禁用二次认证，可为相应管理员开启/禁用二次认证

图 4-6

4.9.4 角色权限 （路径：用户管理-角色权限）

超级管理员可对角色进行查看、新增、编辑、删除操作。对于不同的角色，超级管理员可以可以自主选择配置此角色的相关权限。

5 附件

附件一 垃圾邮件投递到邮箱垃圾邮件文件夹配置方法

（需要在邮箱系统端做相关配置）

一、Coremail邮箱系统配置方案

1. 新增关键字规则，配置匹配到信头条件时投递邮件到垃圾箱；优先级最低，如图1

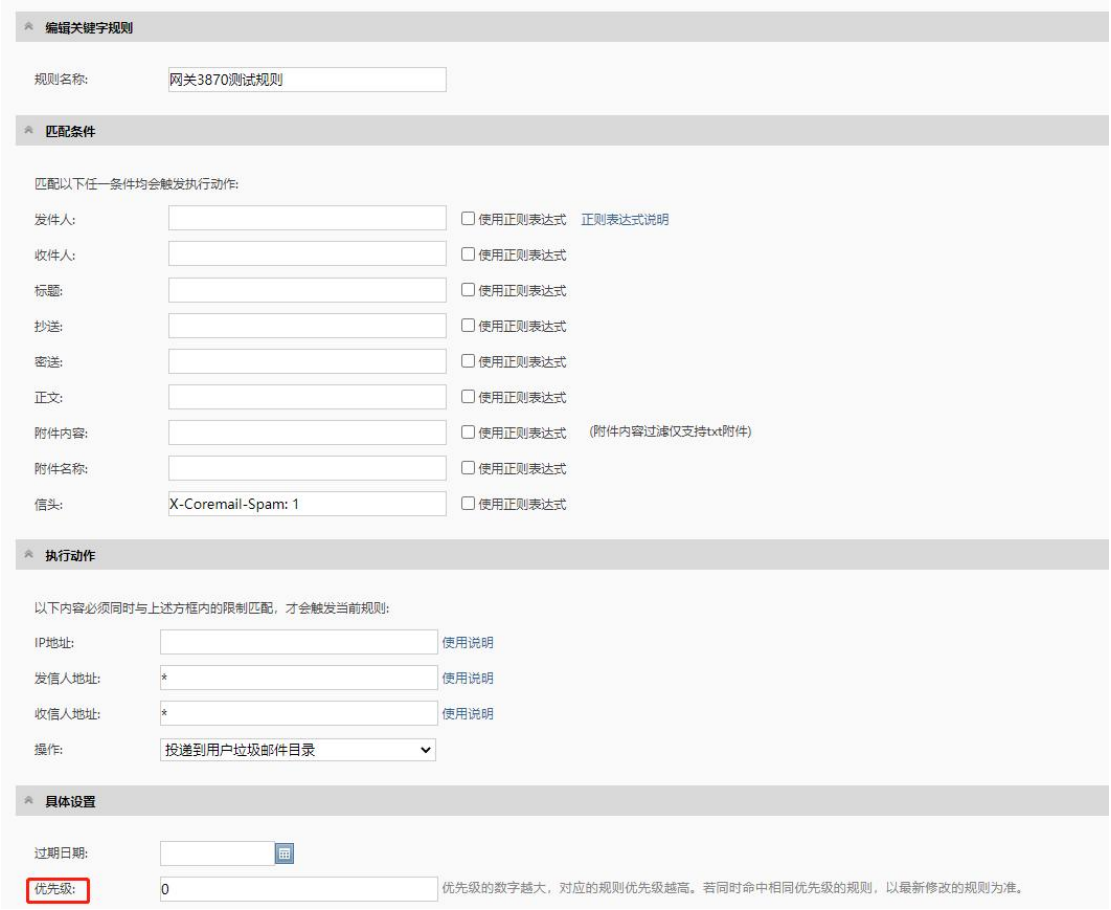


图1

2.增加发信人策略，如 图2—图7


编辑发信人策略
策略名称:网关3870测试用策略
具体设置
基本设置
出错次数控制
IP连接频率控制
用户发送邮件频率控制
过滤分数阈值设置
高级设置
收件人个数限制(来自外站):
-1
外站邮件投递到本站时的收件人个数限制（-1表示无限制）
重置为默认值
发信人非本站用户时发送邮件大小上限:
-1
KB （-1表示无限制,0表示立即销毁）
重置为默认值
当Mail From命令的内容为空时:
接受
当Mail From使用不存在的用户或者非法用户时:
接受
重置为默认值
是否忽略SMTP验证:
是
重置为默认值

图2


编辑发信人策略
策略名称:网关3870测试用策略
具体设置
基本设置
出错次数控制
IP连接频率控制
用户发送邮件频率控制
过滤分数阈值设置
高级设置
每个连接SMTP认证失败次数上限:
-1
(-1表示无限制,0表示立即销毁)
重置为默认值
每个连接可以接受的命令次数上限:
-1
(-1表示无限制,0表示立即销毁)
重置为默认值
每个连接可以接受的命令错误次数上限:
-1
(-1表示无限制,0表示立即销毁)
重置为默认值

图3

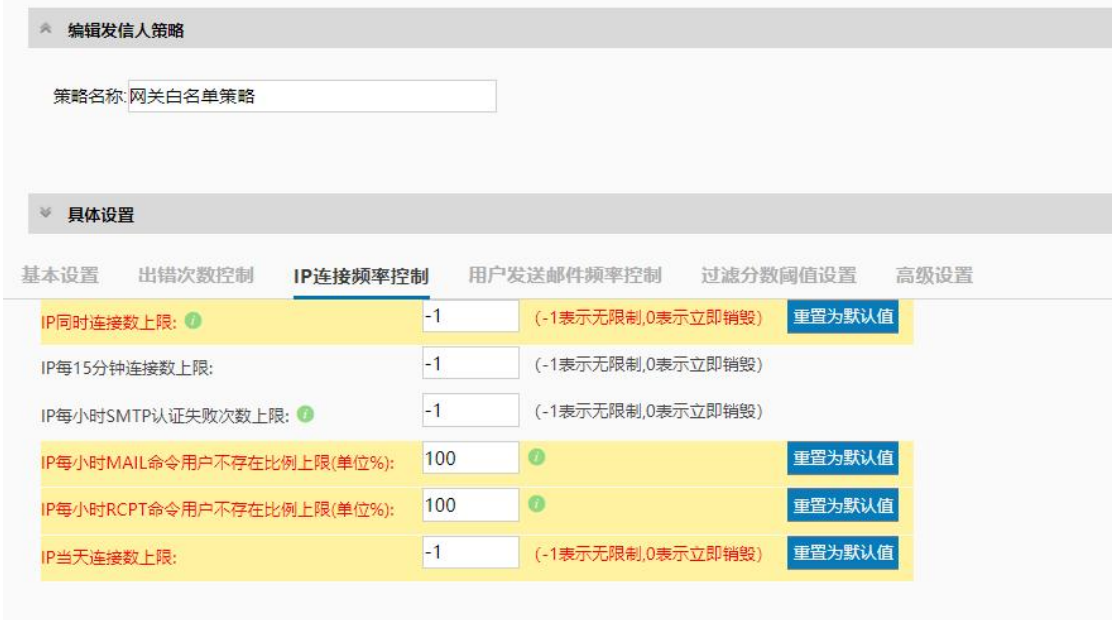

编辑发信人策略
策略名称:网关白名单策略
具体设置
基本设置
出错次数控制
IP连接频率控制
用户发送邮件频率控制
过滤分数阈值设置
高级设置
IP同时连接数上限:
-1
(-1表示无限制,0表示立即销毁)
重置为默认值
IP每15分钟连接数上限:
-1
(-1表示无限制,0表示立即销毁)
IP每小时SMTP认证失败次数上限:
-1
(-1表示无限制,0表示立即销毁)
IP每小时MAIL命令用户不存在比例上限(单位%):
100
重置为默认值
IP每小时RCPT命令用户不存在比例上限(单位%):
100
重置为默认值
IP当天连接数上限:
-1
(-1表示无限制,0表示立即销毁)
重置为默认值

图4


编辑发信人策略
策略名称:网关3870测试用策略
具体设置
基本设置
出错次数控制
IP连接频率控制
用户发送邮件频率控制
过滤分数阈值设置
高级设置
用户每15分钟发出邮件的总数上限:
-1
(-1表示无限制,0表示立即销毁)
重置为默认值
用户当天发出邮件的总数上限:
-1
(-1表示无限制,0表示立即销毁)
重置为默认值
用户每15分钟发出邮件中收信人总人次上限:
-1
(-1表示无限制,0表示立即销毁)
用户当天发出邮件中收信人总人次上限:
-1
(-1表示无限制,0表示立即销毁)

图5


编辑发信人策略
策略名称:网关3870测试用策略
具体设置
基本设置
出错次数控制
IP连接频率控制
用户发送邮件频率控制
过滤分数阈值设置
高级设置
反垃圾功能将根据设定分值对所有邮件进行过滤，各分区的分值需填写范围为0-100的整数
外站用户发给本站用户
灰名单过滤分值(默认7,使用灰名单技术阻隔邮件):
100
重置为默认值
标记分值(默认100,邮件主题加上标记前缀):
100
垃圾邮件分值(默认10,把邮件保存到用户的垃圾邮件文件夹):
100
重置为默认值
阻断分值(默认100,直接reject此邮件):
100
是否过滤本站发出的邮件:
否

图6

图7

3.增加发信人规则，IP填网关的IP，对应使用4中的发信人策略，如图8

图8

4. 在邮箱系统的配置文件修改发件人策略的CAC检查开关：

NeedCACCheckBySystemRule="true" # 默认为false

5. 邮箱系统的FreeIP去掉网关的IP，配置项在programs.cf FreeIPList；

6. 去掉邮箱系统对网关的发信人白名单

二、Exchange邮箱系统配置方案

1. Exchange邮箱系统需要添加的规则，如图9：

   "X-Coremail-Spam" 头包含 "1"，将SCL设为”9“

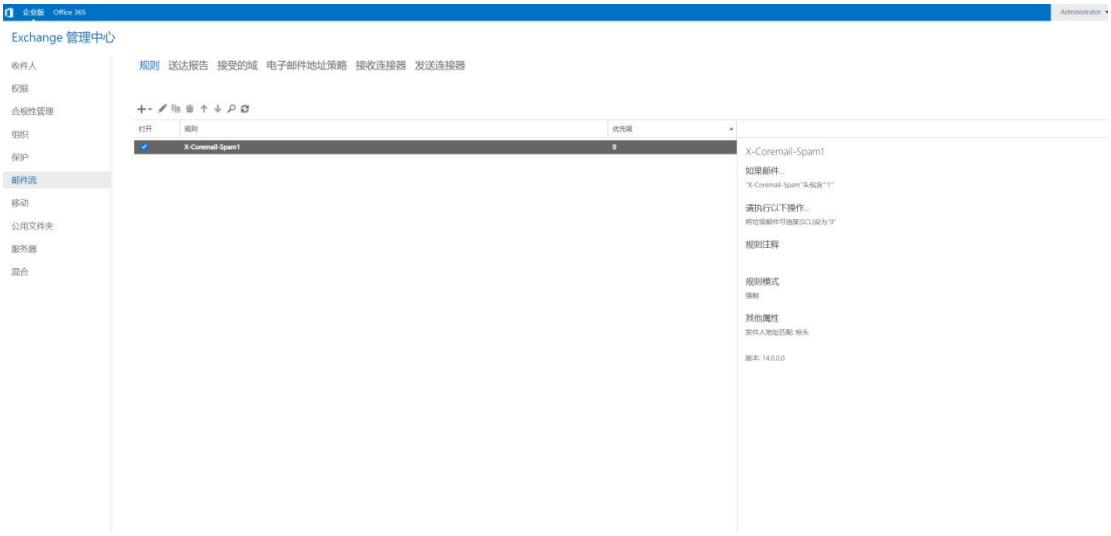


图9

2. Echange配置SCL方法： https://docs.microsoft.com/zh-cn/exchange/configure-anti-spam-settings-on-mailboxes-exchange-2013-help