

Barracuda SpamFirewall User Guide

梭子鱼垃圾邮件防火墙用户手册

REV 1.0.0

博威特网络技术(上海)有限公司 技术部

概述	6
1. 梭子鱼垃圾邮件防火墙技术特点	6
2. 图示	6
3. 动态更新实现最大保护和简单管理	7
4. 接收过滤和外发模式	8
5. 技术支持	8
6. 保证	8
一、 垃圾邮件防火墙型号	8
1. 表格	9
二、 本文档相关信息	9
1. 基本设置	9
2. 过滤设置	10
3. 用户设置	10
4. 域设置	11
5. 高级设置	11
三、 首次安装	12
1. 开箱确认	12
2. 安装时需要的其他设备	12
3. 安装梭子鱼垃圾邮件防火墙	12
4. 配置系统IP地址和网络设置	13
5. 配置你公司的出口防火墙	13
6. 配置梭子鱼垃圾邮件防火墙	13
7. 配置管理选项	15
8. 更新系统软件	15
9. 验证你的动态更新许可状态	15
10. 将接受的外部邮件路由到梭子鱼垃圾邮件防火墙	16
11. 调整默认的垃圾过滤设置	17
四、 安装示例	17
1. 梭子鱼垃圾邮件在公司出口防火墙后面	17
2. 梭子鱼垃圾邮件防火墙在DMZ区	18
五、 操作模式	19
1. 将梭子鱼垃圾邮件防火墙工作模式转换成外发模式。	19
2. 将外发模式转换成接收过滤模式	21
六、 基本设置	22
状态	22
1. 监控系统状态	22
2. 使用状态页面	22
3. 邮件统计	22
4. 性能统计	23
5. 许可状态	23
6. 每小时和每天的邮件统计	24
7. 理解指示灯状态	24
邮件日志	24
1. 监控邮件日志	24

2.	使用指导.....	25
3.	邮件分类.....	25
4.	邮件日志概述.....	26
5.	改变邮件日志显示属性.....	27
6.	显示邮件详细信息.....	27
7.	删除邮件日志.....	27
	垃圾邮件评分.....	28
1.	配置垃圾邮件评分标准.....	28
2.	指定主题文本和被标记邮件的优先级.....	28
3.	向发件人发送通知信.....	28
	病毒扫描.....	29
1.	启用和禁用病毒扫描及通知发件人.....	29
	邮件隔离.....	29
1.	设置隔离策略.....	29
2.	指定隔离类型.....	30
3.	指定全局隔离设置.....	30
4.	指定每用户隔离设置.....	30
	IP地址配置.....	31
1.	配置系统IP信息.....	31
	系统管理.....	32
1.	管理接口的访问控制.....	32
2.	改变管理用户的密码.....	32
3.	对管理接口和API的限制访问.....	32
4.	改变管理界面的语言.....	33
5.	允许邮件正文在邮件日志显示.....	33
6.	改变WEB接口的端口和会话超时.....	33
7.	系统关机.....	33
8.	使用前面板重启系统.....	34
9.	系统告警的自动发送.....	34
10.	改变系统的工作模式.....	34
	贝叶斯/意图分析.....	35
1.	允许邮件客户端对邮件进行分类.....	35
2.	使用Outlook和Lotus Notes插件.....	36
3.	管理贝叶斯数据库.....	36
4.	重置贝叶斯数据库.....	36
5.	发送垃圾邮件到博威特网络.....	36
6.	启用意识分析.....	37
	关闭弹回通知.....	37
7.	附加信息.....	37
七、	过滤设置.....	38
1.	设置黑名单服务.....	38
2.	黑名单服务的描述.....	38
3.	如果你公司的域或者IP地址在黑名单之内将会发生什么.....	39
4.	IP地址过滤.....	39

5.	发送者的域过滤.....	40
6.	发送者邮件地址过滤.....	40
7.	接受者邮件地址过滤.....	40
8.	附件过滤.....	41
9.	主题过滤.....	42
10.	信体过滤.....	42
11.	信头过滤.....	43
八、	用户设置和域设置.....	43
1.	梭子鱼垃圾邮件防火墙如何创建用户.....	43
2.	查看用户帐户.....	43
3.	使用过滤条件来查看帐户.....	44
4.	编辑用户帐户.....	45
5.	删除无效的用户帐户.....	45
6.	为帐户指定相关选项设置.....	45
7.	添加或更新用户帐户的隔离设置.....	46
8.	设置邮件策略.....	46
9.	管理你的隔离信箱.....	47
10.	添加新域.....	50
11.	编辑域.....	50
12.	设置LDAP.....	51
九、	高级设置.....	53
1	邮件协议.....	53
2	速率控制.....	54
3	限定用户.....	54
4	配置备份.....	55
5	外观设置.....	57
6	Syslog日志.....	58
7	信任转发.....	58
8	外发页脚.....	59
9	IP高级配置.....	59
10	集群管理.....	60
11	单点登陆.....	62
12	SSL设置.....	62
13	区域关键字.....	63
14	通知邮件编辑.....	64
15	诊断工具.....	65
16	报表管理.....	65
17	SMTP/TLS.....	66
18	任务管理.....	67
19	恢复控制台.....	67
十.	梭子鱼外发模式.....	68
附一.	梭子鱼常见问题Q&A.....	74
	什么是垃圾邮件评分，贝叶斯学习，邮件指纹识别？.....	74
	全局隔离设置与分用户隔离设置的根本不同是什么？.....	74

全局和分用户垃圾邮件隔离概要什么时候发出?	74
能够同时选择全局和分用户两种隔离类型吗?	74
除了通过web界面访问垃圾邮件防火墙操作系统外, 是否还有别的方式如telnet或ssh?	74
可否配置梭子鱼能将分类为垃圾的邮件复本投递到一个邮箱中? (不为隔离, 仅为转移)	74
能否设置垃圾邮件防火墙能够针对发件人DNS域进行反垃圾检查?	75
如何更新垃圾邮件规则和病毒特征码?	75
梭子鱼垃圾邮件防火墙对域的支持数量有限制吗?	75
梭子鱼垃圾邮件防火墙能否设置多域过滤邮件。.....	75
能否将博威特垃圾邮件防火墙与邮件服务器设置在不同的子网中。.....	75
为什么WEB管理界面上梭子鱼防火墙的更新及动态更新都没升级?	75
高级页防火墙更新中出现如下信息是什么意思?	76
梭子鱼防火墙前面板上的指示灯标示似乎与灯的指示含义不符?	76
梭子鱼垃圾邮件防火墙(BSF) 安装完成后会不会造成邮件收发延时?	76
梭子鱼垃圾邮件防火墙使用的是何种病毒引擎。.....	77
什么是DoS和DDoS攻击?.....	77
我有问题怎么和梭子鱼的技术支持取得联系?	77
我无法打开机器的“邮件日志”?	77
我的界面是英文的, 并且无法升级到中文?	77
我在第一个页面看到的系统性能统计数据页中, 发现有部分红色部分绿色的条框, 请问 是什么意思?	78
我的邮箱帐号是否保存在梭子鱼机器内, 如果梭子鱼产品当机, 是否会影响我的邮件帐 户的正常使用?	78
梭子鱼要求SMTP握手是什么意思?	78
何谓梭子鱼的意图分析/目的分析?	79
分用户隔离设置是怎么回事?	79
梭子鱼中关于使用表达式的说明.....	80
贝叶斯过滤是如何评分的?.....	82
附二. 常见错误邮件信息列表.....	83
附三. 常见有限保修、快速替换和动态更新服务问题解答	85
动态更新服务.....	85
有限保修.....	85
快速替换服务.....	87
补充条例.....	88
附四 梭子鱼垃圾邮件防火墙标准服务条款.....	89

概述

1. 梭子鱼垃圾邮件防火墙技术特点

梭子鱼垃圾邮件防火墙是可以提供强大的,可扩展的垃圾邮件和阻断病毒的集成了硬件和软件的设备,并且它不会降低邮件服务器的性能。本系统不需要每用户的许可费且可升级至支持几万个活动邮件用户。

你可以使用基于 web 的管理接口配置十二个防护层来保护你的用户以避免受到垃圾邮件和病毒邮件的影响。这十二个防护层如下:

- ✚ 防 DOS 攻击和安全保护
- ✚ 速率控制
- ✚ IP 地址信誉评价
- ✚ 发送者验证
- ✚ 接收者认证
- ✚ 病毒检测
- ✚ 策略控制(用户特殊规则)
- ✚ 垃圾邮件指纹检测
- ✚ 实时意图分析
- ✚ 图象分析
- ✚ 贝叶斯过滤分析
- ✚ 基于规则的评分技术

下图显示了这些防护层的检查顺序:

2. 图示



3. 动态更新实现最大保护和简单管理

动态更新以达到最少的管理和最大程度的保护

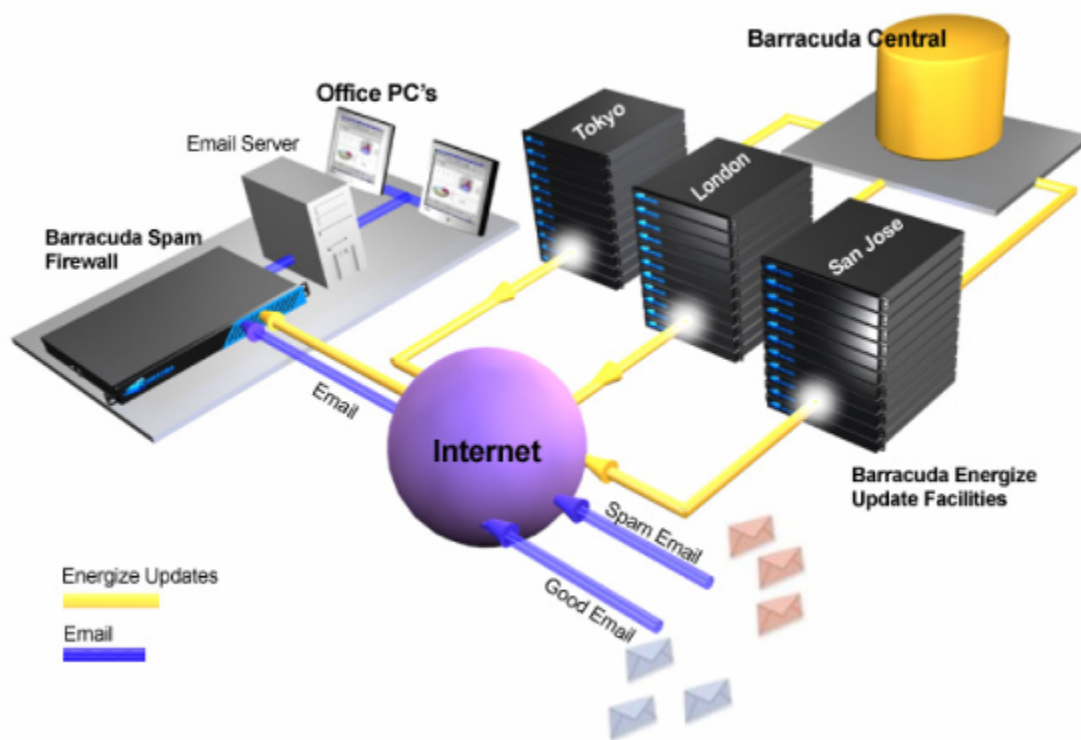
为了给你提供最大程度的保护以免遭最新的垃圾邮件和病毒攻击，梭子鱼网络公司维护了一个强大的梭子鱼中心。梭子鱼工程师监控互联网上垃圾邮件和病毒攻击的趋势，并把这些更新的垃圾邮件规则库和病毒库及时的加入到梭子鱼中心。通过使用梭子鱼的动态更新功能，这些新的更新可以被梭子鱼防火墙自动获得。

通过在早期确定垃圾邮件的趋势，梭子鱼中心的工程团队能够快速开发新的阻断技术和定义病毒。所有这些都可以通过快速服务于你的梭子鱼垃圾邮件防火墙。

动态更新可以给你的梭子鱼垃圾邮件防火墙提供以下益处：

- ✚ 更新已知的 IP 信誉评分表
- ✚ 对于已知的垃圾邮件信息的直接的阻断
- ✚ 对于已知垃圾邮件内容的阻断
- ✚ 更新垃圾邮件规则库
- ✚ 更新已知的病毒定义库
- ✚ 更新梭子鱼内核

下图描述了梭子鱼中心如何通过动态更新来提供最新的垃圾邮件和病毒定义库的方法



理解垃圾邮件评分规则

梭子鱼垃圾邮件防火墙详细检查邮件的所有特征并且使用一个复杂的评分系统来决定邮件是否是垃圾邮件。当一封邮件到达基于评分的策略系统的时候，梭子鱼垃圾邮件防火墙会对邮件的所有属性打分。

例如，梭子鱼垃圾邮件防火墙检查：

- 邮件信头和主题行的攻击性的字符或单词



- 邮件中的 **HTML** 的百分比
- 邮件中是否包含未知的链接

所有这些属性都帮助梭子鱼垃圾邮件防火墙决定邮件的评分结果，在 **web** 管理接口的邮件日志页面里可以查看这些信息。

动态更新保持了最新的垃圾邮件规则和评分系统，使垃圾邮件防火墙能够快速抵制垃圾邮件发送者的最新技术。

4. 接收过滤和外发模式

梭子鱼垃圾邮件防火墙能够配置成如下两种工作模式之一：

-  接收过滤（默认）对所有进入的邮件进行病毒和垃圾邮件的扫描，这种模式确保所有发送到你的用户的邮件是合法的且没有病毒。
-  外发模式对所有外发的邮件（从你的用户）进行病毒和垃圾邮件的扫描。这种模式确保所有从你的网络中外发的邮件是合法的且没有病毒。

你的梭子鱼垃圾邮件防火墙只能工作于两种模式中的一种。默认的，所有出货的梭子鱼垃圾邮件防火墙被配置成接收过滤模式。

关于如何把梭子鱼垃圾邮件防火墙配置成外发模式，请参考[把你的系统配置成外发模式](#)此页。关于外发模式的特殊功能，请参考第 **recovery console** 章。

5. 技术支持

联系梭子鱼网络公司技术支持：

- 请拨打电话+86 21 5452 0358/0368 转 技术支持
- 也可以发送电子邮件到support@barracudanetworks.com.cn

6. 保证

对于设备制造上的问题，梭子鱼垃圾邮件防火墙有 90 天的退换货担保。

一、 垃圾邮件防火墙型号

梭子鱼垃圾邮件防火墙有各种型号。每种型号的容量和特性请参考下表：

1. 表格

特性	200 型号	300 型号	400 型号	600 型号	800 型号	900 型号
活动邮件用户	1-500	300-1000	1000-5000	3000-10000	8000-22000	18000-25000
支持域	50	250	500	5000	5000	5000
兼容所有邮件服务器	是	是	是	是	是	是
系统安全加固	是	是	是	是	是	是
垃圾邮件阻断	是	是	是	是	是	是
病毒扫描	是	是	是	是	是	是
基于 web 界面的管理	是	是	是	是	是	是
外发模式	是	是	是	是	是	是
TLS 加密支持	是	是	是	是	是	是
SSL 支持	是	是	是	是	是	是
每用户设置和隔离	否	是	是	是	是	是
MS Exchange/LDAP 加速	否	是	是	是	是	是
Syslog 支持	否	是	是	是	是	是
SNMP/API	否	否	是	是	是	是
每域设置	否	否	是	是	是	是
集群支持	否	否	是	是	是	是
RAID 支持	否	否	是	是	是	是
每用户评分设置	否	否	否	是	是	是
可自定义外观	否	否	否	是	是	是
RAID 热插拔支持	否	否	否	否	是	是
网络存储支持	否	否	否	否	否	是

二、 本文档相关信息

这个部分列出了管理界面中的每个页面的相关主题

1. 基本设置

下面是基本设置页面里的相关主题

管理界面	相关设置
------	------

状态	监控系统状态
邮件日志	监控邮件日志
垃圾邮件评分（必须是接收过滤模式）	配置全局垃圾邮件评分 指定主题文本和标记邮件的优先级别
病毒检查	启用或禁用病毒检查和通知
隔离	设置隔离策略
IP 地址配置	配置系统的 IP 地址
管理	管理接口的访问控制 关闭系统 系统告警和通知的自动发送 改变系统的工作模式
贝叶斯和意图分析（必须是接收过滤模式）	让用户在客户端分类邮件 管理贝叶斯数据库 启用意图分析

2. 过滤设置

下面是过滤设置页面里的相关主题

管理界面	相关。。
外部黑名单（必须是接收过滤模式）	预定黑名单服务
IP 过滤	IP 地址过滤
发送者的域过滤	发送者的域过滤
发送者的过滤	发送者的地址过滤
接受者的过滤	接受者邮件地址的过滤
附件的过滤	附件类型过滤
主题过滤	主题行的过滤
邮件信体过滤	信体的过滤
信头过滤	信头的过滤

3. 用户设置

下表列出了用户页面的相关主题。这里的设置在外发模式下或者 200 型号上不可以使用。

查看帐户	浏览用户帐户 编辑用户帐户 删除无效的帐户
用户特征	为用户帐户分配可用功能
添加用户/更新	特定用户的隔离设置
用户备份/恢复	从备份文件恢复
保留策略	设置保留策略

4. 域设置

这个设置对于 200/300 型号的设备只有部分功能。

管理界面	相关...
域管理	添加域 编辑域 使用 LDAP 为用户认证

5. 高级设置






下面是过滤设置页面里的相关主题

管理界面	相关主题
邮件协议	修改邮件协议设置
限速	配置邮件速度限制
外发用户（必须是接收过滤模式）	激活个人帐户
备份	备份和恢复系统配置
动态更新	更新垃圾邮件规则库和病毒库
软件更新	更新系统软件版本
外观（必须是接收过滤模式）	自定义管理界面的外观（200/300 型号不支持）
Syslog 日志	使用日志服务器管理系统日志
外发/转发（接收过滤模式支持）	设置可信转发和 SASL/SMTP 认证
输出脚本	自定义输出脚本
高级 IP 配置（接收过滤模式支持）	高级 IP 地址配置
集群	设置集群和备用系统
单点登录（接收过滤模式支持）	配置单点登录
SSL	启用 SSL 功能
区域设置	中文和日文的垃圾邮件检测
弹回邮件设置	自定义不发送报告
故障排除	故障排除
报表	生成系统报表
SMTP/TLS	通过 TLS/SSL 启用 SMTP 认证
任务管理	使用任务管理器来监控系统任务

三、 首次安装

1. 开箱确认

非常感谢您购买梭子鱼垃圾邮件防火墙。请按照下列各项来核对箱子中的附件。如果有丢失或者损坏，请联系梭子鱼网络公司销售代表。

-  梭子鱼垃圾邮件防火墙（核对您收到正确的型号）
-  电源线
-  以太网线
-  装配栏杆（只针对 600/800/900 型号）
-  《梭子鱼垃圾邮件防火墙用户手册》 一本

2. 安装时需要的其他设备

安装梭子鱼垃圾邮件防火墙时需要这些设备


- VGA 显示器
- PS2 键盘

3. 安装梭子鱼垃圾邮件防火墙


把梭子鱼垃圾邮件防火墙固定起来

-  固定梭子鱼垃圾邮件防火墙到一个标准的 19 英寸的架子上或者其他的稳定的位置。

警告：不要遮挡设备前面和后面的通风孔。

-  用 5 类双绞线通过梭子鱼垃圾邮件防火墙后面的以太网端口把他连接到你网络的交换机上。梭子鱼垃圾邮件防火墙支持以太网 10M 和 100M 的速度，梭子鱼网络公司推荐使用 100M 的以太网连接以达到最佳性能。不要使用电缆连接设备的其他端口，这些端口在诊断时才使用。

注意：梭子鱼垃圾邮件防火墙 600 和 800 型号的可以支持千兆以太网，且有两个 LAN 端口。安装这种型号时，请把以太网电缆插入到第二个 LAN 端口。

-  把下面附件连接到您的梭子鱼垃圾邮件防火墙上：

- 电源线
- 显示器
- 键盘

-  按下设备前面板的电源按钮启动系统

显示器有管理控制的登录提示，系统前面的指示灯已经点亮。每个指示灯代表的意义请参考 *理解指示灯的含义*。

4. 配置系统 IP 地址和网络设置

梭子鱼垃圾邮件防火墙的默认 IP 地址是 192.168.200.200。你可以通过下面任何一种方法来改变：

1. 通过控制接口直接连接梭子鱼垃圾邮件防火墙来指定一个新的 IP 地址
2. 按住前面板上的 reset 按钮不要松开。保持 5 秒，就将 IP 地址改变为 192.168.200.200。按住 reset 按钮保持 8 秒，就将 IP 地址改变为 192.168.1.200。按住 reset 按钮保持 12 秒，就将 IP 地址改变为 10.1.1.200。。

直接连接到梭子鱼垃圾邮件防火墙上设置新的 IP 地址：

- ✚ 在梭子鱼垃圾邮件防火墙提示登录时，输入用户 admin 和秘密 admin 登录。用户确认请求窗口将显示当前的系统 IP 配置。
- ✚ 使用 tab 键，选择 yes 来改变 IP 地址
- ✚ 输入新的 IP 地址，子网掩码和默认网关后并选择 ok。
- ✚ 当提示你是否想改变 IP 地址时选择 yes。保存后新的 IP 地址和网络设置就被应用到梭子鱼垃圾邮件防火墙上。

5. 配置你公司的出口防火墙

如果你的梭子鱼垃圾邮件防火墙位于你公司防火墙的后面，你就需要指定特殊的端口来允许梭子鱼垃圾邮件防火墙与远程服务器的通信。

配置你的公司防火墙：

1. 下表作为参考。在你公司防火墙上打开以下端口。

端口	方向	协议	目的
22	In	TCP	远程诊断和技术支持 (可选)
25	In/out	TCP	SMTP(必需)
53	Out	TCP/UDP	DNS
80	Out	HTTP	病毒库，系统软件和 垃圾邮件规则库更新 (必需)
123	In/out	UDP	NTP

2. 如果需要的话，在你公司防火墙上改变 NAT 路由将进入的邮件路由到梭子鱼垃圾邮件防火墙上。参考你公司防火墙的文档或者请教你公司防火墙的管理员来做必要的修改。

6. 配置梭子鱼垃圾邮件防火墙

在指定了系统的 IP 地址和开放你公司防火墙上必要的端口后，你需要从管理接口来配置梭子鱼垃圾邮件防火墙。确认配置梭子鱼垃圾邮件防火墙的电脑连接到相同的网络，并且配

置合适的路由以便允许通过 web 浏览器连接到梭子鱼垃圾邮件防火墙。

配置梭子鱼垃圾邮件防火墙：

1. 在浏览器中输入梭子鱼垃圾邮件防火墙的 IP 地址，端口是 8000

例如：http://192.168.200.200:8000

2. 输入用户 admin 和密码 admin 登录到管理界面
3. 选择基本设置->IP 配置，输入需要的相关信息

下表描述了你需配置的区域

TCP/IP 配置	你的梭子鱼垃圾邮件防火墙的 IP 地址，子网掩码，默认网关 梭子鱼垃圾邮件防火墙接受进入邮件的 TCP 端口。默认是 25
目的邮件服务器 TCP/IP 设置	你的目的邮件服务器的主机名或者 IP 地址，例如 mail.yourdomain.com.这个邮件服务器是邮件在病毒和垃圾扫描后的接受邮件服务器。 你最好指定你邮件服务器的名称而不要指定 IP 地址。这样是为了在移动邮件服务器或是任何时候 DNS 的更新时，不需要改变梭子鱼垃圾邮件防火墙的任何配置。 TCP 端口是目的邮件服务器接受任何 SMTP 流量（如，进入邮件）的端口。默认是 25。 如果你需要安装一个以上的域或者邮件服务器，请参考添加新城
DNS 配置	输入你网络上的主备 DNS 服务器地址。 强烈推荐你指定一个主 DNS 和一个备份 DNS 服务器。梭子鱼垃圾邮件防火墙的一些特征，（比如假冒发送者的域检测）依靠于 DNS 的可用性。
域配置	默认的主机名是梭子鱼垃圾邮件防火墙回复邮件的地址里使用的主机名（不发送给接受者，病毒警告通知等）
允许收件人域名	这些域是梭子鱼垃圾邮件防火墙所管理的。确认填写好这个列表。梭子鱼垃圾邮件防火墙拒绝所有邮件地址不是这个列表内的进入的邮件。 如果需要允许所有经过梭子鱼的域发送到你的邮件服务器，请在这里输入一个星号*。 注意：一个梭子鱼垃圾邮件防火墙能支持多个域和邮件服务器。如果你有多个邮件服务器，请到域配置页面，输入每个域关联的邮件服务器。

4. 点击 save 保存按钮，保存设置。

如果你改变了梭子鱼垃圾邮件防火墙的 IP 地址，你就会断开同管理接口的连接。你需要使用新的 IP 地址重新登录。

7. 配置管理选项

设置管理选项：

1. 选择基本设置->系统管理
2. 为梭子鱼垃圾邮件防火墙设置新的管理密码
3. 设置本地时区。梭子鱼垃圾邮件防火墙上的时间是通过 NTP 来自动更新的，这个协议使用的是 123 端口，所以需要在你的公司防火墙上开放 123 端口（入和出双向开放）。
注意：正确设置时区是很重要的，因为它决定了邮件的发送时间并且可能出现在邮件阅读程序里。
4. 点击 save 保存按钮。

8. 更新系统软件

在更新梭子鱼垃圾邮件防火墙之前，建议您阅读发行通知。

更新梭子鱼垃圾邮件防火墙的系统软件：

1. 选择高级设置->软件更新
注意：在下载新版本的系统软件之前要知道发行备注。发行备注为你提供了新版本的最新特性和改正。你可以访问发行备注信息通过“高级配置->系统软件升级->查看版本信息”
2. 点击“现在下载”
3. 想看到下载进程，在点击 refresh 刷新按钮后就可以看到完成百分比。一旦下载完成，那个按钮就会变成现在应用。Apply now
注意：应用过程将需要几分钟的时间。在下载的时候一定要不能断电。当在下载的时候，进入和发出邮件的流量是不会中断的。
4. 点击 apply now 来激活刚刚下载的系统软件。这个过程结束后会自动重新启动系统并立刻导致你 web 接口连接断开。这是正常的，也是预期的行为。所有不需要手动重启系统。Web 接口在 5 分钟后又可以重新使用，您需要重新登录。

9. 验证你的动态更新许可状态

当你安装梭子鱼垃圾邮件防火墙的时候，你的动态更新和立即更换预定是激活的。验证许可的状态是非常重要的，这样你梭子鱼垃圾邮件防火墙可以从梭子鱼中心接受到最新的病毒库和垃圾邮件规则库。动态更新服务对于下载病毒库和垃圾邮件规则库到你的系统上是可靠的。

检查你的许可状态：

1. 选择基本设置->系统状态

2. 在许可状态区域，验证在动态更新和更换服务的旁边有单词“使用中”如果购买的话。下图显示了许可状态的位置

有一个新的系统版本可以升级 最新版本: 3.4.10.086

	总计	今天	本小时
阻断	75,687	1,625	84
阻断: 病毒	392	0	0
隔离	3,560	60	2
允许: 标记	6,311	71	5
允许	25,882	582	23
总共收到邮件	111,832	2,338	114

许可证

规则库升级: 未被激活 (点击此处激活)

立即替换: 不购买

性能统计

In/Out 邮件队列: 0/4

平均反应时间: 59 秒

最后邮件: 3 分钟前

唯一收件人: 343

系统负荷: 1%

CPU 风扇速度: 7031 RPM

系统风扇速度: 3590 RPM

CPU 温度: 39 °C

系统存储: 44%

邮件日志存储: 25%

每小时邮件统计

■ 允许
■ 允许: 标记
■ 隔离
■ 阻断: 病毒
■ 阻断: 垃圾邮件

3. 如果许可状态是未被激活的，请安下面操作。

请打开下面的注册网址进行注册: <http://www.barracudanetworks.com.cn/register.htm>

10. 将接受的外部邮件路由到梭子鱼垃圾邮件防火墙

安装梭子鱼垃圾邮件防火墙的下一步是把进入的邮件路由到系统上，以便于它能够对进入的邮件进行病毒和垃圾邮件的扫描。你可以使用以下任意一种方法把邮件路由到梭子鱼垃圾邮件防火墙上：

- ✚ **端口转发**当梭子鱼垃圾邮件防火墙位于运行 NAT 的公司防火墙后面时使用。
- ✚ **MX 记录**当具有可路由公网 IP 地址的梭子鱼垃圾邮件防火墙位于 DMZ 区域时使用。
注意：不要通过梭子鱼垃圾邮件防火墙路由由外发邮件。只有你将梭子鱼垃圾邮件配置成转发模式或者使用梭子鱼垃圾邮件的外发模式时，才把邮件路由到梭子鱼垃圾邮件防火墙上。

在你将进入邮件路由到梭子鱼垃圾邮件防火墙之后，它就会过滤接受到的所有邮件并将合法的邮件路由到你的邮件服务器上。

✧ 端口转发

当你的梭子鱼垃圾邮件防火墙位于公司防火墙之后时，你需要做一个端口重定向（也叫端口转发），将进入的 SMTP 流量（端口时 25）指向梭子鱼垃圾邮件防火墙上。

更多关于端口转发的信息，请参考你公司的防火墙文档或者询问管理员。

◇ MX 记录

如果你梭子鱼垃圾邮件防火墙位于 DMZ 区（不受到你公司防火墙的保护），按照以下方法将进入的邮件路由到系统上。

1. 为你的梭子鱼垃圾邮件防火墙创建一个 DNS 记录
下面的例子显示了一个 IP 地址是 66.233.233.88，名称是 barracuda 的垃圾邮件防火墙的 DNS 记录：
Barracuda.yourdomain.com IN A 66.233.233.88
2. 改变你的 DNS MX 记录
下面的例子显示了一个优先级为 10 的相关 MX 记录
IN MX 10 barracuda.yournetwork.com

11. 调整默认的垃圾过滤设置

在你安装梭子鱼垃圾邮件防火墙之后，系统开始基于默认设置来过滤进入的邮件。例如，设备会自动对进入的邮件进行病毒检查和使用梭子鱼的黑名单服务来识别垃圾邮件。

一开始，你的梭子鱼垃圾邮件防火墙被配置成，将邮件主题行添加单词“BULK”的邮件标记为最有可能是垃圾邮件。一旦你更熟悉梭子鱼垃圾邮件防火墙时，你就能轻松自如的调整系统处理垃圾邮件。例如，你可能不会阻断垃圾邮件而选择隔离它。

当你第一次调整系统设置时，一般的设置如下所示：

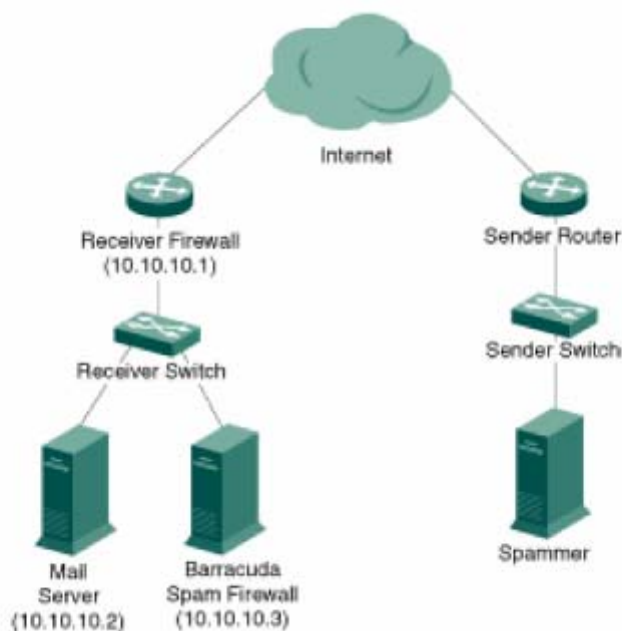
任务	参考
监控和分类进入的邮件	分类邮件
验证默认的垃圾邮件评分设置	配置全局垃圾邮件评分值
设置隔离（可选）	设置隔离策略
对来自指定的 IP 地址，域或邮件帐户的邮件进行阻断	使用阻断和接受过滤

四、 安装示例

这部分提供了一个安装示例，在你把梭子鱼垃圾邮件防火墙安装到公司网络时可以作为参考。

1. 梭子鱼垃圾邮件在公司出口防火墙后面

下图显示了把垃圾邮件防火墙安装在你公司网络防火墙之后。在这个例子中，邮件服务器的 IP 地址是 10.10.10.2,垃圾邮件防火墙的 IP 地址是 10.10.10.3。

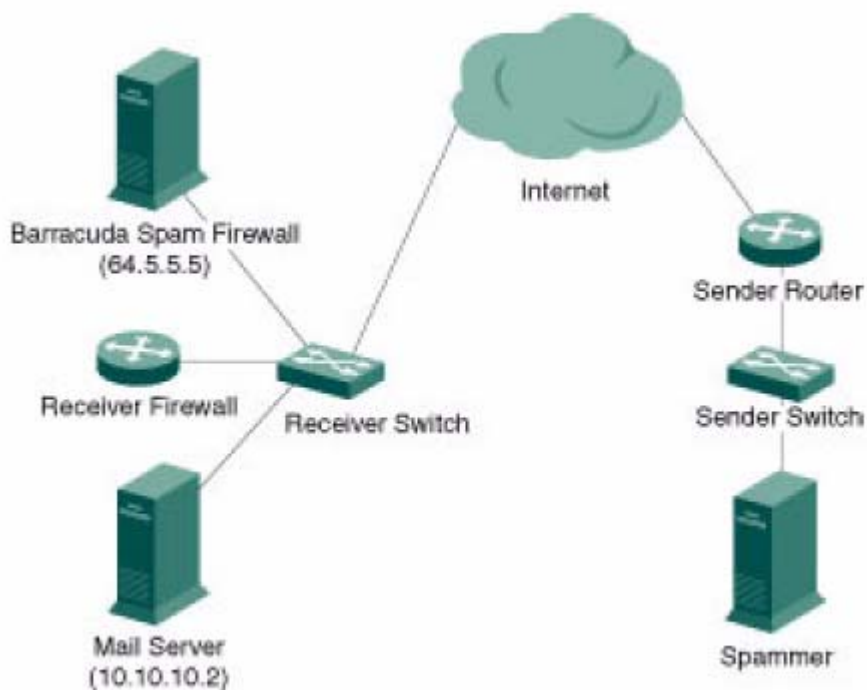


在这种安装类型，请完成以下任务：

- 1) 转发（端口重定向）25 端口的进入的 SMTP 流量到垃圾邮件防火墙（10.10.10.3）上。
 - 2) 配置垃圾邮件防火墙转发过滤后的邮件到目标邮件服务器（10.10.10.2）上。
- 这种安装类型不需要修改任何 MX 记录。

2. 梭子鱼垃圾邮件防火墙在 DMZ 区

下图显示了将垃圾邮件防火墙安装在你公司防火墙之前（在 DMZ 区域中）。在这个例子中，邮件服务器的 IP 地址是 10.10.10.2，垃圾邮件防火墙的公共 IP 地址是 64.5.5.5。



这种安装类型，需完成以下任务：

- 1) 给梭子鱼垃圾邮件防火墙分配一个可用的外部的公共 IP 地址。
- 2) 在 DNS 服务器上改变 MX 记录，将流量指向到垃圾邮件防火墙上。在 DNS 服务器上为垃圾邮件防火墙创建 A 记录和 MX 记录。

下面显示了名称为 barracuda，IP 地址是 64.5.5.5 的垃圾邮件防火墙一个 DNS 记录。



```
Barracuda.yourdomain.com IN A 64.5.5.5
```

下面显示了优先级为 10 的相关联的 MX 记录。

```
IN MX 10 barracuda.yournetwork.com
```

五、 操作模式

梭子鱼垃圾邮件防火墙能够配置成如下两种工作模式之一：



-  接收过滤模式（默认）对所有进入的邮件进行病毒和垃圾邮件的扫描。
-  外发模式对所有外发的邮件（从你的用户）进行病毒和垃圾邮件的扫描。
这种模式确保所有从你的网络中外发的邮件是合法的且没有病毒。

最常用的模式是接收过滤模式，这种模式可以对进入的邮件进行病毒和垃圾邮件的扫描。如果你公司想对员工外发的邮件进行扫描的话，你可以将系统配置成外发模式。

如果希望对进入和外发的邮件都进行扫描，你可以把垃圾邮件防火墙配置成接收外发一体化模式。这种模式是启用“外发特性”的接收过滤模式。这种“基本的外发”模式将不会标记或隔离任何外发的邮件。它将只对所有的的外发邮件执行基本的病毒扫描，同时对所有进入的邮件进行完全的病毒和垃圾邮件扫描。

1. 将梭子鱼垃圾邮件防火墙工作模式转换成外发模式。

梭子鱼垃圾邮件防火墙只能工作在一种模式下。如果你从接收过滤模式改变到外发模式，请注意以下：

-  **系统所有的邮件日志和隔离邮件将被删除。**
-  系统配置会保留。但是，你应该核实那些配置对外发模式是否合适。

改变垃圾邮件防火墙的模式：

- 1) 选择基本设置->系统管理。
- 2) 在操作模式部分，点击 转变。
- 3) 点击确认按钮，确认你想改变垃圾邮件防火墙的工作模式。一个状态条显示了垃圾邮件防火墙的转变过程。一旦转换完成，你的垃圾邮件防火墙会自动重启。

下面是系统重启后的一些设置。

一、 基本设置

在系统重启后，登录到垃圾邮件防火墙上再检查一下用户接口的变化。

- 1) 选择基本设置->IP 配置
- 2) 在 TCP/IP 配置部分验证垃圾邮件防火墙的 IP 地址，子网掩码和默认网关。垃圾邮件防火墙接受进入邮件的 TCP 端口，默认是 25。

- 3) 在 DNS 配置部分检查你网络的 DNS 设置。梭子鱼垃圾邮件防火墙的一些特性依赖于可靠的 DNS，比如发件人域欺骗检查。
- 4) 在域配置部分，验证主机名称和域名称必须是正确的。这个名称是从垃圾邮件防火墙发送邮件（未发送给接受者，病毒警告通知等）时使用的。
- 5) 如果你已经完成配置，请点击保存配置。

二、 把你的邮件服务器设置为 Smart Host 转发主机

转变垃圾邮件防火墙到外发模式的最后一步是将内部邮件服务器在发送邮件之前把外发的邮件转发到垃圾邮件防火墙上。通过将你的邮件服务器配置为 Smart Host 转发主机来实现。下面的网站提供了如果将指定的邮件服务器配置为转发主机的指南。其他信息，请询问邮件服务器的管理员和相关文档。

邮件服务器类型

E-mail 服务器	参考
Microsoft exchange server 2003	http://support.microsoft.com/kb/265293
Novell groupwise server	http://www.novell.com/documentation/gw55/index.html?page=/documentation/gw55/gw55ia/data/a2zi22h.html
Lotus Domino Server	http://www.12.lotus.com/lidd/doc/domino_notes/Rnext/help6_admin.nsf/f4b82fbb75e942a6852566ac0037f284/14cdfcaa188fa90a85256c1d003955af?OpenDocument

启用智能主机 smart host

- a) 使用 KVM 连接到内部邮件服务器（10.0.10.10）
- b) 打开桌面主机的**系统管理器 system manager**
- c) 选择管理组->第一管理组->服务器->cuda-server->协议->SMTP
- d) 右键点击默认的 SMTP 连接器，选择属性
- e) 点击**发送页面 delivery tab**
- f) 点击高级按钮
- g) 在 Smart Host 主机区域输入垃圾邮件防火墙的 IP 地址
- h) 点击 OK
- i) 再次点击 OK，退出
- j) 从第八步重复第三步设置剩下的 SMTP 连接器（ST1-ST6）

禁用 Smart Host 主机

- a) 使用 KVM 连接到内部邮件服务器（10.0.10.10）
- b) 打开桌面主机的**系统管理器 system manager**
- c) 选择管理组->第一管理组->服务器->cuda-server->协议->SMTP
- d) 右键点击默认的 SMTP 连接器，选择属性
- e) 点击**发送页面 delivery tab**
- f) 点击高级按钮
- g) 删除 **smart host 下的任何内容**

- h) 点击 OK
- i) 再次点击 OK, 退出
- j) 从第八步重复第三步设置剩下的 SMTP 连接器 connector (ST1-ST6)

2. 将外发模式转换成接收过滤模式

当你从外发模式转变回接收过滤模式时, 请注意以下几点:

- 1) **系统所有的邮件日志和隔离邮件将被删除。**
 - 2) 系统配置会保留。但是, 你应该核实那些配置对接收过滤模式是否合适。
如果希望对进入和外发的邮件都进行扫描, 你可以把垃圾邮件防火墙配置成混合模式。这种模式是启用“外发特性”的接收过滤模式。这种“基本的外发”模式将不会标记或隔离任何外发的邮件。它将只对所有的邮件执行基本的病毒扫描, 同时对所有进入的邮件进行完全的病毒和垃圾邮件扫描。
- ### 改变垃圾邮件防火墙的工作模式
- 1) 选择基本设置->系统管理。
 - 2) 在操作模式部分, 点击 转变。
 - 3) 点击确认按钮, 确认你想改变垃圾邮件防火墙的工作模式。一个状态条显示了垃圾邮件防火墙的转变过程。一旦转换完成, 你的垃圾邮件防火墙会自动重启。

基本配置

在系统重启后, 登录到垃圾邮件防火墙上再检查一下用户接口的变化。

- 1) 选择基本设置->IP 配置
- 2) 在 TCP/IP 配置部分验证垃圾邮件防火墙的 IP 地址, 子网掩码和默认网关。垃圾邮件防火墙接受进入邮件的 TCP 端口, 默认是 25。
- 3) 在 DNS 配置部分检查你网络的 DNS 设置。梭子鱼垃圾邮件防火墙的一些特性依赖于可靠的 DNS, 比如发件人域欺骗检查。
- 4) 在域配置部分, 验证主机名称和域名称是正确的。这个名称是从垃圾邮件防火墙发送邮件 (未发送给接受者, 病毒警告通知等) 时使用的。
- 5) 确认梭子鱼垃圾邮件防火墙列出了被管理的允许邮件接受者的所有的域。垃圾邮件防火墙拒绝所有邮件目标地址不在这个列表中的进入邮件。
- 6) 如果你已经完成配置, 请点击保存配置。

重新检查管理设置

- 1) 选择基本设置->系统管理
- 2) 检查系统管理设置没有被改变
- 3) 如果你改变了设置, 请保存。

设置基本的转发

如果你希望垃圾邮件防火墙既过滤进入的邮件又过滤外发的邮件, 那么你需要设置为接收过

滤模式并且启用设置你的邮件服务器作为转发主机所描述的“转发”特性，并且设置可信任的转发和 SASL/SMTP 认证。注意，这种模式不会标记或隔离任何外发的邮件，只对转发到梭子鱼垃圾邮件防火墙的外发邮件执行基本的扫描。

将进入和外发的邮件路由到梭子鱼垃圾邮件上

设置垃圾邮件防火墙的最后一步是把进入和外发的邮件路由到系统上，这样它就可以对进入的邮件进行病毒和垃圾邮件的扫描。更多信息，请参考[路由进入的邮件到梭子鱼垃圾邮件防火墙上](#)。

P36

六、 基本设置

状态

1. 监控系统状态

通过以下步骤你可以监控垃圾邮件防火墙的状态：

- 基本设置->状态页面（管理界面中）
- 系统前面板的指示灯

2. 使用状态页面

基本设置->状态页面提供了梭子鱼垃圾邮件防火墙的当前状态和性能的总览。从这页你可以看到：

- 邮件统计显示了有多少邮件被阻断，隔离，标记和允许了。
- 性能统计
- 许可状态
- 每小时和每小时统计

3. 邮件统计

统计	描述
阻断	系统阻断的病毒和垃圾邮件的数量
阻断：病毒	系统阻断的病毒邮件数量
隔离	系统隔离的邮件数量。默认的，系统不隔离邮件。 <i>如需启用隔离功能，请参考</i>

	设置隔离策略。
允许：标记	系统标记的邮件数量。标记邮件的主题行是基于在垃圾邮件评分页面里设置的。
允许	被发送到目的接受者的邮件数量。这些邮件没有被阻断或是修改。
总数	自从系统安装或是最后复位时所有的邮件统计数量。
今天	今天的邮件统计数（从 00:00—00:00）。
本小时	本小时的邮件统计。例如，如果现在是上午 10:45，那么统计的时间是从 10:00 到 10:45。

4. 性能统计

统计	描述
In/out 邮件队列	是以比率显示的，比如 10/5。第一个数字代表进入邮件的数量，这包括等待进行病毒和垃圾邮件扫描的邮件。第二个数字代表邮件队列里外发的数量。点击进入和外发的数字，你可以看到当前邮件队列的概要。
平均反应时间	系统进行标记，隔离，发送邮件花费的时间。
最后邮件	最后被发送出去的邮件的时间
CPU 风扇速度	Cpu 风扇的速度
Cpu 的温度	Cpu 的温度
唯一收件人	在 24 小时之内接受邮件的“唯一收件人”。这个数量不包括被拒绝的接受者。
系统负荷	评估系统的 cpu 和硬盘的负荷。100% 系统负荷是异常的，尤其是进队列非常大的时候。长时间系统的负荷都在 100%，足以说明存在内部系统问题，特别是进队列继续在增长。
冗余 (RAID)	RAID 系统的状态。200 和 300 型号的机器没有冗余统计。
系统存储	不同系统模块使用的存储空间的使用率。
邮件日志存储	邮件和日志存储空间的使用率。

系统和邮件日志存储显示了每个分区上被使用的百分比率。当这两个分区中的任意一个使用率达到 90% 时，梭子鱼垃圾邮件防火墙会发出系统警告。如果一个分区达到了极限，请联系梭子鱼公司技术支持。

5. 许可状态

这部分表明了许可证是否有效或过期：

动态更新

立刻替换（可选服务）

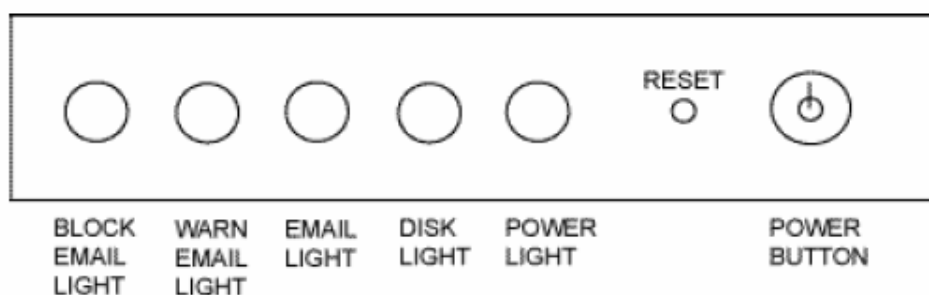
如果其中之一或是两个许可都过期了，请联系梭子鱼公司售后服务部来更新你的许可证。

6. 每小时和每天的邮件统计

显示了前 24 小时和前 25 天里被阻断，隔离的邮件数量。

7. 理解指示灯状态

梭子鱼防火墙前面板有 5 个指示灯，当系统处理邮件时这些灯会闪烁。



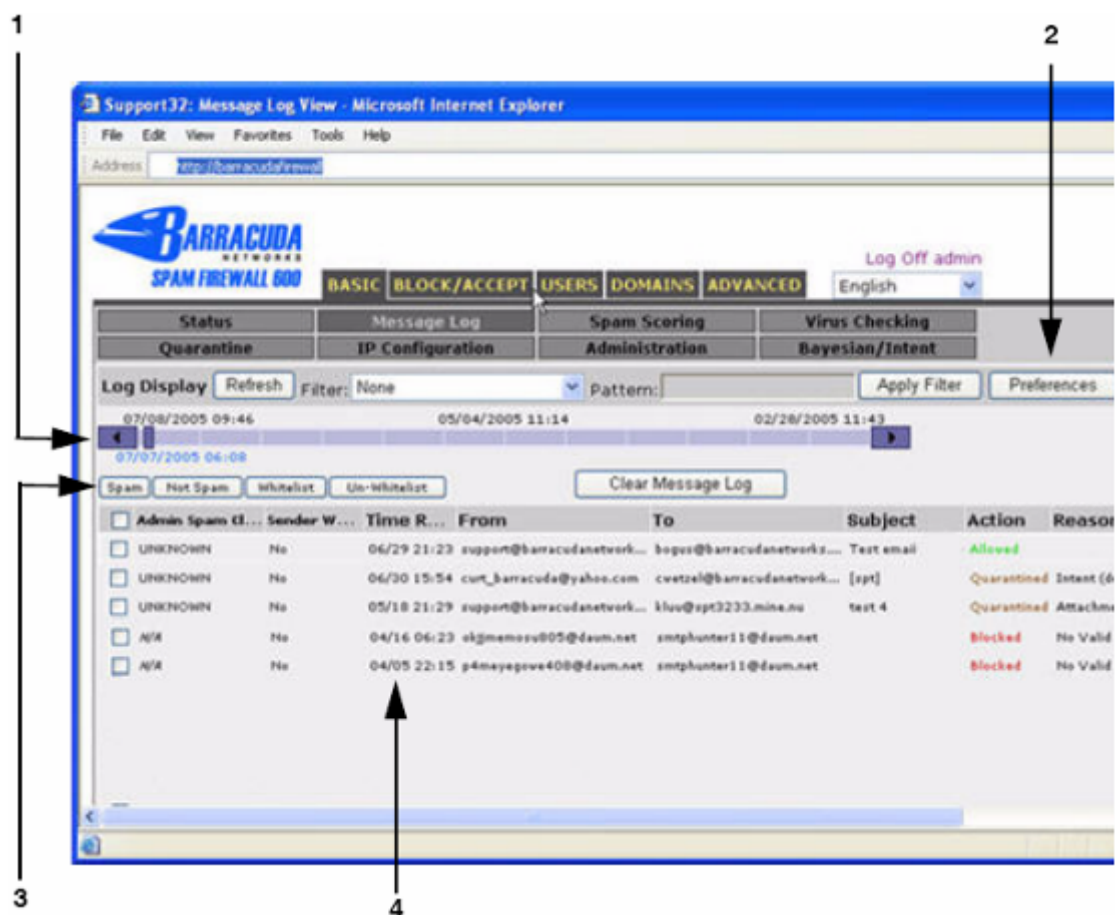
灯	颜色	描述
阻断邮件	红	当阻断垃圾邮件或病毒邮件时闪烁
警告邮件	黄	当邮件被标记为垃圾邮件或隔离时闪烁
邮件	绿	当设备收到邮件时闪烁
硬盘	绿	硬盘工作时闪烁
电源	绿	系统接通电源时持续绿灯

邮件日志

1. 监控邮件日志

建议经常在邮件日志里监控进入的邮件。尽可能多的将邮件分类为垃圾邮件或正常邮件，也可以将邮件加入到白名单中。

分类邮件可以在贝叶斯数据库中建立规则，梭子鱼按照这个规则来处理以后的邮件。下图显示了在邮件日志中的一些主要按钮。



2. 使用指导

这是对于上图的相关解释：

- 1 时间区域可以让你根据时间来选择邮件日志。
- 2 显示属性可以让你自己定义邮件日志的显示方式
- 3 分类按钮可以让你将邮件分为正常邮件或是垃圾邮件，也可以将发送者添加到白名单中。
- 4 列出了所有邮件日志，你可以点击其中一个记录来显示邮件细节。

3. 邮件分类

分类邮件来建立规则是梭子鱼垃圾邮件防火墙处理进入邮件的最简单的方法。下表列出了在邮件日志页面里的常用按钮。

按钮	描述

垃圾邮件	在贝叶斯数据库中将该邮件分类为垃圾邮件，贝叶斯数据库在超过 200 封垃圾邮件或者 200 封正常邮件被分类之后启动，此时梭子鱼垃圾邮件防火墙开始扫描邮件寻找匹配项目，影响邮件的评分。如果分用户隔离启用，被每一位用户操作的邮件分类，也将加入到贝叶斯数据库。查看目前被分类为垃圾邮件的数量，到基本--->贝叶斯/指纹页面。
正常邮件	在贝叶斯数据库中将该邮件分类为正常邮件。贝叶斯数据库在超过 200 封垃圾邮件或者 200 封正常邮件被分类之后。此时，梭子鱼垃圾邮件防火墙开始扫描邮件寻找匹配项目，影响邮件的评分如果分用户隔离启用，被每一位用户操作的邮件分类也将加入到贝叶斯数据库。查看目前被分类为垃圾邮件的数量，到基本--->贝叶斯/指纹页面
白名单	将此邮件的发件人加入到你的白名单。从白名单发件人收到的邮件不进行垃圾邮件评分。从白名单发件人收到的邮件依然经过病毒扫描，附件类型过滤，信头、新体及主题内容的阻断过滤。
白名单删除	将邮件的发件人从你的白名单删除。
清除日志	清除所有显示的日志。这不将清除你为收到邮件设定规则的贝叶斯数据库。这不会删除贝叶斯数据库数据。

4. 邮件日志概述

以下表格说明在邮件日志表格中每栏目的作用

垃圾邮件分类	指示邮件被分类为垃圾邮件或非垃圾邮件。当你在邮件日志头的按钮标记一个邮件是垃圾邮件或者非垃圾邮件时，该分类在栏目中出现。
列入白名单	确认发件人在你的白名单中。所有从你的白名单发件人发到的邮件是允许的，除非检测到病毒，或者邮件包含一个不允许的附件类型。
日期	梭子鱼垃圾邮件防火墙收到邮件的日期
自/致	发件人及收件人的邮件地址
主题	邮件主题行的内容
原因	采用动作的原因，如发件人在你的黑名单上，或者邮件被识别为垃圾邮件。在一些情况下，此栏目可能显示“邮件大小”做为邮件被许可的原因。当此原因显示时，表示梭子鱼垃圾邮件防火墙并没有扫描垃圾邮件因为该邮件超过 100K。很少有垃圾邮件超过这个大小限制，而扫描垃圾邮件可能性极小的大邮件大大降低系统资源使用的有效性。
评分	邮件的垃圾邮件评分。该评分从 0（一定不是垃圾邮件）到 10 或者以上（一定是垃圾邮件）
来源 IP	发件人的 IP 地址或者主机名
发送状态	输出队列中邮件的状态，是否已经被发送到了目的服务器。
发送细节	邮件的发送状态细节
ID	显示了邮件的唯一识别号码

查看邮件	查看完整的邮件
查看源文件	查看邮件源文件
动作	邮件被处理的方式（允许，标记，阻断，隔离）
接受时间	梭子鱼垃圾邮件防火墙接受到邮件的时间

5. 改变邮件日志显示属性

你可以点击右边“显示属性”来改变邮件日志的显示格式。你可以：

- 隐藏你不想显示的列
- 改变每列的显示顺序，这样重要的列在前面显示
- 增加或减小每列的宽度
- 改变每页显示的邮件的数量
- 从本梭子鱼垃圾邮件防火墙上显示邮件（集群环境）。邮件日志默认是显示你集群环境中所有垃圾邮件防火墙上的邮件。如果“只显示当前的邮件”被设置为“是”的话，那么邮件日志将不会显示集群中另外一个垃圾邮件防火墙上的邮件。管理员只可以对当前显示邮件进行分类。相反的，管理员不能对集群中其他系统的邮件分类，因为管理员没有登录到那个系统。

6. 显示邮件详细信息

在邮件日志页面，你可以点击一个邮件来查看邮件的详细信息。你可以看到：

- 查看邮件 查看邮件的内容
- 查看源文件 查看邮件的源文件
- 发送 发送此邮件到目的地

查看邮件的信体可以帮助你识别单词或字符，这些单词和字符可以添加到信体过滤中。例如：如果看到很多邮件正文中有“as seen on TV”，那么你可以添加“as seen on”作为关键词来阻断，隔离或标记包含这些单词的邮件。

如果由于隐私的原因，你不想让邮件的正文被显示，你可以选择隐藏信体内容。在基本设置一》系统管理页面里设置。

7. 删除邮件日志

点击“清除邮件日志”按钮将会删除所有的邮件日志，但是不会删除贝叶斯数据库。从系统硬盘上完全删除邮件日志可能会花费 2 小时到 4 天。在这个时间内，磁盘的处理速度会变慢。

垃圾邮件评分

1. 配置垃圾邮件评分标准

一旦邮件通过了过滤检测，它就有一个垃圾邮件可能性的评分。这个评分范围是从 0 到 10 的，0 定义为正常邮件，10 定义为垃圾邮件。

垃圾邮件防火墙是基于这个分数来对邮件进行标记，隔离，阻断或是允许的。下表描述了在基本设置—》垃圾邮件评分里如何设置的。如果你设置为 10 分，则会禁用此项。

注意：在梭子鱼 400 或以上型号，你可以在域设置里设置每个单独域的垃圾邮件评分。

设置	描述
标记 分值	当邮件得分超过以上的限度，但是小于隔离限度，邮件将被在主题栏插入[BULK]后发送给收件人。你可以在垃圾邮件标记设置部分修改插入主题栏的缺省字符。任何低于该得分的邮件将自动被许可，缺省值是 3.5。
隔离 分值	当邮件得分超过以上的限度，但是小于阻断限度，邮件将被转发到你界定的隔离信箱。要了解指定隔离信箱的信息，参阅全局隔离设置。缺省设置是 10（系统不隔离邮件）。启用隔离功能，此设置必须有一个低于阻断限度的值。
阻断 分值	当邮件得分超过以上限度，邮件将不被发给收件人，一个无法发送收条（NDR）或者弹回信息将由梭子鱼垃圾邮件防火墙发给发件人（可以在下面的弹回信选项中设置是否发送这个 NDR 信息），这个数值默认是 7。

2. 指定主题文本和被标记邮件的优先级

基础—>垃圾邮件评分页使你能够输入你希望加入主题行起始处的文字。缺省的文字是“[BULK]”，系统将在以下情况标记一个邮件：

- 该邮件的垃圾邮件评分超过了标记限度（低于隔离限度）
- 过滤器发现一个应该被标记的邮件。更多的设定过滤器的信息，请查看过滤设置。

如果“设置低优先级”被选为是，所有被标记的或隔离的邮件设置为低优先级。默认情况下，梭子鱼垃圾防火墙由于评分或内容阻断邮件时会通知发送者。如要关闭自动通知发件人，设置“发送弹回通知信”为“否”

3. 向发件人发送通知信

垃圾邮件弹回配置

这个选项决定了由于垃圾邮件评分或是内容过滤而阻断邮件时是否向发件人发送一个通知信。在所有的配置都验证完之后，应该将此项设置为“是”。

病毒扫描

1. 启用和禁用病毒扫描及通知发件人

在梭子鱼上，病毒扫描是自动启用的，系统会定时更新病毒库（默认是每小时）。

基本设置一》病毒扫描 按下表来配置病毒扫描和通知发件人。修改后请点击保存修改。

设置	说明
病毒扫描	当病毒扫描启用，所有邮件将自动扫描病毒。一个扫描出病毒的邮件将被阻断。它不会被隔离也不会发给目标收件人，甚至收件人已列入白名单。建议你启用病毒扫描。注意：在梭子鱼垃圾邮件防火墙 400 及 600 型号，你能够在高级-->高级域设置页为你的每个域分别启用及禁用病毒扫描。为了更多信息，参阅系统日志服务器中央管理系统日志。
病毒通知	启用病毒通知时，如果邮件包含一个病毒梭子鱼垃圾邮件防火墙会通知目标收件人。推荐你将“通知发件人病毒截获”设置为否，防止梭子鱼垃圾邮件防火墙在大规模病毒爆发时发送大量的通知信件，不但占有大量带宽而且令使用者厌烦。

邮件隔离

1. 设置隔离策略

缺省状态下，梭子鱼不配置为隔离邮件。但是启用隔离的话，可以增加安全性。和标记邮件不同，隔离邮件不会被发送到目的收件人，因为这样可以避免用户打开被感染的邮件并在你的网络中传播病毒。在你的系统上设置隔离功能：

在外发模式的系统上启用隔离，请参考外发模式。

- 1) 使用垃圾邮件评分来启用隔离，在基本设置一》垃圾邮件评分页面。
请参考配置垃圾邮件评分。
- 2) 选择基本设置一》隔离设置
- 3) 选择隔离类型
对全局隔离类型，请输入全局隔离发送地址。
对分用户隔离类型，配置分用户隔离设置
- 4) 点击保存修改

2. 指定隔离类型

隔离类型决定了梭子鱼垃圾邮件防火墙是否将隔离邮件发送到全局隔离地址或是用户的隔离信箱。

注意：如果你的梭子鱼型号是 400 或以上，你可以指定分域隔离。在域设置一》点击编辑域来设置。

隔离类型	隔离邮件的保存地方	隔离责任
分用户隔离 (200 型号不支持)	将隔离邮件保存在梭子鱼垃圾邮件防火墙上用户的隔离信箱。如果你选择此类型，梭子鱼垃圾邮件防火墙会自动创建用户的隔离信箱。	每个终端用户可以在他们自己的隔离信箱中管理自己的隔离邮件。
全局隔离	发送所有的隔离邮件到你指定的全局发送邮箱（注意这个邮箱是要实际存在的，并且拥有很大的容量）。	梭子鱼垃圾邮件防火墙的管理员管理隔离邮件。

3. 指定全局隔离设置

下表描述了如何设置全局隔离。在基本设置一》隔离设置这个页面

区域	说明
隔离邮件发送地址	指定所有隔离邮件需发送到的邮箱。该邮箱可以在梭子鱼垃圾邮件防火墙保护的服务器（如 youname@yourdomain.com）或者一个远程邮件服务器
隔离邮件主题	

4. 指定每用户隔离设置

下表描述了分用户隔离的配置。在基本设置一》隔离设置页面。这部分不适用于梭子鱼 200 型号。

设置	描述
隔离回复地址	这个地址是所有用户收到隔离通知的 from 地址。如果用户回复通知信的话，邮件会被发送到这个邮箱中。
隔离主机	所有隔离通知被发送到用户的 IP 地址或主机名，这样他们可以访问隔离信箱。此区域空白将采用梭子鱼垃圾邮件防火墙当前的 IP 地址为隔离主机。如果你的用户需要一个外部 IP 地址登陆服务器，梭子鱼垃圾邮件防火墙没有设置一个，你需要选择另一台服

	务器做为隔离主机，并在区域内填入哪台服务器的外部地址。
隔离默认状态	<p>隔离帐户创建时的缺省状态</p> <p>如果被设置为“是”，所有新用户使用分用户隔离功能。如果被设置为“否”，用户不会在他们的隔离信箱中收到邮件。邮件的主题行会被标记一个隔离主题，并被发送到用户的信箱中。</p> <p>假如只为部分用户启用分用户隔离功能（但其他用户禁用此功能），设置此项为否。</p>
域连接	<p>这个设置决定了不同的域是否使用相同的分用户设置和隔离信箱。</p> <p>如果设置为是，相同的分用户设置和隔离信箱被所有相同名称的邮件地址使用，但这个用户属于不同的域。例如：启用域连接，someuser@yourdomain.com，someuser@yourdomain.net，和someuser@corp.yourdomain.com将会共享相同的设置和隔离信箱。注意以下特征：</p> <ul style="list-style-type: none"> ➤ 域连接是一个全局设置。你不能只为几个域或几个用户设置域连接。 ➤ 如果邮件地址属于相同的域，这个功能将不起作用。例如：someuser@yourdomain.com不能链接到some.user@yourdomain.com。
通知间隔	梭子鱼通知用户被隔离邮件的间隔
通知时间	梭子鱼发送隔离通知的时间（以 hh:mm 格式）。这个修改将在第二天生效。

IP 地址配置

1. 配置系统 IP 信息

基本设置->IP 设置包含了梭子鱼设备的设置和你的邮件服务器的设置。

项目	描述
测试配置（只支持接收过滤模式）	点击开始测试，可以验证你的梭子鱼上 IP 信息是否正确。并生成一个状态报告显示了测试的结果（这个测试并不适用于大部分国内防火墙映射的客户，它的测试只对梭子鱼和邮件服务器都直接设置公网 IP 地址的 ISP 机房内用户比较准确）。
TCP/IP 配置	<p>梭子鱼的 IP 地址，子网掩码，默认网关。TCP 端口是梭子鱼接受进入邮件的端口。通常是 25 端口。</p> <p>注意： 如果你的梭子鱼运行版本是 3.1.x 或更早，并且是集群环境的一部分，</p>
目标邮件服务器 TCP/IP 配置(接收过滤模式)	你目标邮件服务器的主机名及 IP 地址，如 mail.yourdomain.com 。这是邮件服务器检查垃圾邮件及病毒后接收邮件的邮件服务器。推荐你指定邮件服务器的主机名而不是 IP 地址，这样目标邮件服务器可以被转移，及更新 DNS，而不需要任何修改梭子鱼设置。TCP 端口是目标邮件服务器接收邮件的端口，通常是 25 端口。
DNS 配置	列出你在网络上使用的主及从 DNS 服务器，强烈推荐你指定一个主及从 DNS 服务器。很多梭子鱼的重要检测模块，如 RBL，虚假发件人域检测等，都需要 DNS 的支持。

代理服务器配置（可选，接收过滤模式）	如果你的梭子鱼设备在代理服务器的后面，你需要输入以下参数。这样你的系统可以下载 firmware 并且能够动态更新。 服务器名称/IP—代理服务器的名称或 IP 地址。 TCP 端口—客户端的认证端口通常是 8080。 用户名—分配给梭子鱼的代理用户名。 密码—分配给梭子鱼的密码。
域配置	默认主机名是回复邮件（未发送到接受者，病毒警告通知等）中使用的主机名。缺省域是用于回复邮件地址的域名（不可发送收件人、病毒警告通知等）
允许邮件收件人域	列出被梭子鱼管理的域。梭子鱼拒绝列表域以外的邮件。允许所有经过梭子鱼的域，在此区间加入星号（*）。 注意：一个梭子鱼防火墙可以支持多个域和多个邮件服务器。如果你有多个邮件服务器，请到域设置这个页面，点击编辑域，为每个域设置不同的邮件服务器。

系统管理

1. 管理接口的访问控制

这个部分描述了通过基本设置—》系统管理页面可以完成的任务。

- ◆ 改变管理员帐户的密码
- ◆ 改变时区
- ◆ 改变 Web 管理界面的默认语言和编码
- ◆ 改变 web 管理接口的端口和会话超时时间
- ◆ 改变邮件日志的私有属性，以决定是否显示邮件信体
- ◆ 改变系统警告和通知的邮件地址
- ◆ 将梭子鱼模式从进入改成外发
- ◆ 重启和关闭系统，重入队列，重新载入设置。

2. 改变管理用户的密码

在系统管理界面里，你可以改变访问此管理接口的密码。输入相关信息后，请保存。

3. 对管理接口和 API 的限制访问

基本设置—》系统管理允许你限制访问梭子鱼管理接口和 API 的 IP 地址范围，或者与梭子鱼建立 SNMP 连接。

设置	描述
管理 IP/范围	这是用户可以访问管理接口的地址范围。在这个范围之外的用户试图访问梭子鱼，将返回无效登录错误。
允许 SNMP 和 API 的 IP 地址范围（接收过滤模式）	在这个地址范围的用户可以通过 API,SNMP 访问梭子鱼设备。更多关于 API 的信息，请参考梭子鱼网站里的 support - 》documentation 。

附加信息：

- ◆ 添加一个单独的 IP 地址，请使用掩码 255.255.255.255
- ◆ 如果你没有指定任何 IP 地址或地址区间的话，所有 IP 系统都可以访问梭子鱼设备。

4. 改变管理界面的语言

如果你使用分用户隔离，那么你的用户登录梭子鱼后可以通过在窗口右边下拉菜单里选择一个语言。梭子鱼支持的语言包括中文，日文，西班牙文，法文等等。你选择的语言只应用到个人隔离接口，不会影响其他用户接口。

5. 允许邮件正文在邮件日志显示

你可以允许信体在邮件日志中显示出来。推荐设置为“是”。

6. 改变 WEB 接口的端口和会话超时

在基本设置—》系统管理界面改变设置

设置	描述
Web 接口的 HTTP 端口	从 web 浏览器访问管理接口的端口（默认是 80）。你可以输入新的端口号，保存修改后请重新登录。
会话超时	用户登录梭子鱼后，超过这个时间会注销（默认是 60 分钟）。可以自己设置。

7. 系统关机

在基本设置—系统管理页面，你可以关闭，重启梭子鱼系统或重新载入设置。

警告： 关闭，重启，重新载入设置会导致邮件发送的暂时中断。

8. 使用前面板重启系统

你可以使用前面板的 reset 按钮来完成：

- ◆ 重新启动系统
- ◆ 将系统 firmware 退回到工厂版本

不要常时间按住 reset 按钮，因为这样会改变系统的 IP 地址。

按下及按住重启按钮达 8 秒钟，将系统缺省 IP 修改为 192.168.1.200,按下及按住重启按钮达 12 秒，IP 地址修改了为 10.1.1.200。

9. 系统告警的自动发送

在基本设置—》系统管理页面，你可以配置让梭子鱼自动把系统状态和系统警告发送到你指定的邮件地址中。填写好地址请保存。系统状态报告将会显示一天中每小时被阻断的，被隔离的，被标记的以及允许的邮件。

10. 改变系统的工作模式

你的梭子鱼系统可以工作在两种模式：接收过滤模式或外发模式。常用的模式是接收过滤模式，可以对进入的邮件进行病毒扫描和识别垃圾邮件。如果你们公司想对你用户外发的邮件进行扫描，你可以将梭子鱼配置为外发模式。如果你希望对进入和外发的邮件都进行扫描，那么你可以将其配置为混合模式，这种混合模式是将信任转发功能启用的接收过滤模式。这允许对外发邮件进行基本的病毒扫描，对进入的邮件进行完全的垃圾邮件和病毒的扫描。

一个梭子鱼只可以工作在一种模式下。如果你想从接收过滤模式改变到外发模式，请注意：

- ◆ 所有的邮件日志数据和隔离邮件将被删除。
- ◆ 系统配置将会保留，但是请你确认一下各项设置。

改变梭子鱼的模式：

1. 选择基本设置—》系统管理
2. 在运行模式这个部分，点击“切换”按钮
3. 点击 ok，确认改变你梭子鱼的工作模式

将会有有一个状态条显示转变的过程。在完成后，你的梭子鱼会重新启动。

贝叶斯/意图分析

1. 允许邮件客户端对邮件进行分类

- 梭子鱼提供了一个邮件客户端插件，这可以让用户在他们的 outlook 或 lotus notes 客户端中直接将邮件分类为正常邮件或垃圾邮件。另外，可以基于用户自己创建维护一个个人的白名单。
- 用户建立的白名单和邮件分类只针对用户个人的贝叶斯数据库，它不会影响全局贝叶斯数据库。在基本设置—》邮件日志页面可以培训全局贝叶斯数据库。
- 200 型号的梭子鱼防火墙不支持此功能。

设置允许你的用户使用 outlook 或 lotus notes 客户端插件：

1. 在基本设置—》贝叶斯/意图分析页面，设置允许用户下载插件为是
2. 如果你允许 outlook 插件，选择让用户下载的版本

Outlook 插件	描述
版本 1	允许从 microsoft outlook 客户端分类邮件为正常邮件或是垃圾邮件。
版本 2	包含了版本 1 的所有功能，并添加了白名单功能。这个功能可以基于用户的行为自动把邮件地址添加到用户的白名单中。 Outlook 插件版本 2 自动的白名单功能如下： <ul style="list-style-type: none"> ✧ 用户发邮件的接受者 ✧ 用户分类为正常邮件的发送者地址 ✧ 任何用户添加到 outlook 联系人列表中的邮件地址

3. 点击保存

在管理界面登录页的下方会出现一个链接，这样用户就可以下载插件了。如下所示：

The screenshot shows a login form with the following elements:

- Login** header
- Instruction: "Please enter your username and password below. If you are an administrator, please enter your administrator login and password."
- Language:** dropdown menu set to "English (US)"
- Log on to:** dropdown menu set to "realm1"
- Username:** text input field
- Password:** text input field
- Login** button
- A red oval highlights the link: [Get Mail Client Plugins Here](#)

2. 使用 Outlook 和 Lotus Notes 插件

在下载并安装好插件后，用户可以使用他们的 outlook 或 lotus notes 客户旁边的按钮



来分类邮件。第一个按钮（绿色）将邮件分类为正常邮件，第二个（红色）按钮将邮件分类为垃圾邮件。

Outlook 插件版本 2 可自动配置：

- ✧ 接受者和新联系人都会成为白名单邮件地址。
- ✧ 将被分类为垃圾邮件这些移动到 outlook 客户端的已删除文件夹。
- ✧ 被分类为正常邮件的“from 地址”加入到白名单中。

个人可以到 outlook 客户端的工具菜单—》选项—》spam firewall 页面改变 outlook 插件的默认设置。

3. 管理贝叶斯数据库

在基本设置—》贝叶斯/意图分析页面允许你管理贝叶斯数据库。

4. 重置贝叶斯数据库

在基本设置—》贝叶斯/意图分析页面，你可以重置贝叶斯数据库。这个数据库包含了你在邮件日志页面里配置的所有规则，比如你分类的正常邮件和垃圾邮件。如果你想重置贝叶斯数据库，清除你配置的规则，请点击“重置”。

5. 发送垃圾邮件到博威特网络

当你在邮件日志中将邮件分类为垃圾邮件时，梭子鱼防火墙同时将此邮件发送到梭子鱼网络，以便进一步的分析。这样梭子鱼网络公司可以改进动态更新所提供的垃圾邮件规则库和意图分析。

将梭子鱼设置为不向梭子鱼网络发送垃圾邮件，请到基本设置—》贝叶斯/意图分析页面，将发送邮件到梭子鱼网络设置为“否”。

6. 启用意识分析

意图分析将尝试着和已知发送垃圾邮件的 URLs 数据库去比较。启用意图分析，你可以减少你用户接受到包含此类 URLs 的垃圾邮件的数量。

设置	描述
意图分析	包含 URLs 规则库中的 URL 的邮件是否应该被标记，隔离或阻断。选择标记或隔离邮件将会导致系统性能的下降。如果要禁用意图分析，选择“关闭”（不推荐）。
实时意图分析	除了使用每小时动态更新中的 URLs 数据库之外，梭子鱼系统还可以实时的连接梭子鱼网络中心来检查最新的列表且能阻断最新的垃圾邮件。 注意：如果启用此选项由于 DNS 查询将会增加邮件的扫描时间。
免除 URL	从意图分析中排除指定的 URLs。任何包含排除的 URLs 仍然被扫描，但是这些邮件不会阻断，隔离或标记。

关闭弹回通知

默认情况下，梭子鱼系统在阻断邮件时会向邮件的发送者发送一个弹回通知。目的是警告合法的用户，他们的邮件没有被发送到目的接受者。但是，如果对非法来源的邮件发送弹回通知却是没有必要的。发送弹回通知将会增加梭子鱼系统的负载，同时也会产生大量的虚假地址的邮件。如果你的梭子鱼很少阻断合法的邮件，建议你关闭发送弹回通知。

关闭弹回通知：

- 1 关闭病毒警告通知
 - 1.1 打开基本设置—》病毒扫描页面，将病毒警告通知设置为“否”。
 - 1.2 点击保存
- 2 关闭垃圾邮件弹回通知
 - 2.1 打开基本设置—》垃圾邮件评分页面，设置发送弹回通知为“否”。
 - 2.2 点击保存
- 3 关闭阻断附件通知
 - 3.1 在过滤设置—》附件过滤页面，设置阻断附件时通知发件人为“否”。
 - 3.2 点击保存

7. 附加信息

关于如何更好的使用贝叶斯数据库，请参考如下文章：

http://www.barracudanetworks.com/ns/download/Barracuda_Bayes.pdf.

七、 过滤设置

1. 设置黑名单服务

外部黑名单页面（仅接收过滤模式）可以让你订阅不同的黑名单服务。外部黑名单有时称为 DNSBLs 或 RBLs，是潜在的垃圾邮件发送源的地址列表。梭子鱼防火墙使用这些列表来验证你接受到的邮件真实性。如果系统从黑名单列表中接受到一份邮件，那么此邮件可能被阻断，隔离或标记。这些依赖于你的设置。

默认情况下，梭子鱼防火墙使用梭子鱼黑名单和 spamhaus.org 黑名单服务。

黑名单有时会产生误判（合法的邮件也被阻断了）。因为梭子鱼防火墙在拒绝此类邮件时会发送通知信，所以发送者会得到通知并且合法的发送者会重新发送他们的邮件。

订阅黑名单服务不会影响梭子鱼防火墙的性能。通常的查询时间是几个毫秒，所以不会产生延迟。一旦你的梭子鱼防火墙查询到一个黑名单服务，那么这个查询会在你本地 DNSserver 上缓存一段时间，以后的查询是很快。

在过滤设置—》外部黑名单服务设置如下：

梭子鱼黑名单	是否启用梭子鱼网络公司维护的黑名单服务。梭子鱼黑名单包括了大量发送垃圾邮件的服务器。
常用外部黑名单	是否启用梭子鱼系统上建立的黑名单服务，选择后保存。
客户自定义外部黑名单	订阅你想使用的黑名单。在输入外部黑名单后，指定你想执行的动作。完成后点击保存。 <i>请使用可信任的黑名单。</i>
黑名单选项	<ul style="list-style-type: none"> ◇ 检查 RBL 延迟—这个选项决定了当 RCPT TO 给出后是否执行 RBL 检查。如果设置为“是”，在 SMTP 传输过程中给出 RCPT TO 后会进行 RBL 检查。这样在邮件日志中就会出现发送者和接受者信息。如果设置为“否”，在邮件日志中只会显示 IP 信息。 ◇ 使用全信头扫描黑名单—如果设置为“是”，将允许梭子鱼防火墙对邮件信头进行扫描。扫描信头将会由于梭子鱼防火墙需要对每个信头进行 DNS 查找而影响系统的性能。如果从互联网发送来的邮件不是直接到达梭子鱼防火墙时，请启用此功能。

2. 黑名单服务的描述

黑名单服务	描述
-------	----

Sbl.spamhaus.org	Spamhaus 跟踪互联网上的垃圾邮件发送者及其组织，可以对互联网提供可靠的实时反垃圾邮件保护。Spamhaus 与法律执行结构在共同努力识别和追踪全世界的垃圾邮件发送者。
Xbl.spamhaus.org	为了阻止不断增长的非法垃圾邮件，spamhaus 发布了开发阻断列表。这个列表属于第三方开发的实时的基于 DNS 的 IP 地址数据库，包括开放的代理服务器，垃圾邮件引擎内嵌的蠕虫/病毒，和其它垃圾邮件发送者使用的其他类型的特洛伊木马。
Relays.ordb.org	ORDB.org 是开放的转发数据库。ORDB.org 是保存了已经验证的开放的 SMTP 中继主机的 IP 地址。这些主机有可能被不法用户利用来发送垃圾邮件。系统管理员可以通过访问此列表来决定接受或拒绝此类地址的邮件交换。
Bl.spamcop.net	Spamcop 是一个更严厉的垃圾邮件阻断服务提供者，它常常会阻断一些正常的邮件服务器，我们推荐如果你要启用这个黑名单列表的话，使用标记形式。

3. 如果你公司的域或者 IP 地址在黑名单之内将会发生什么

如果你的域或 IP 地址在黑名单中，那么梭子鱼将不会从那个域中的用户发送邮件。你的域在黑名单里，可能有以下几个原因：

- 你的邮件服务器被别人劫持利用来发送垃圾邮件了。
- 你的邮件服务器是一个开放的中继主机，意思是任何未认证的用户都可以使用它来发送邮件。
- 垃圾邮件发送者使用你的域作为一个伪造域来发送垃圾邮件。

注意：如果你的域或 IP 地址在黑名单里，请直接联系黑名单维护者，让他们将其删除。

4. IP 地址过滤

你可以基于发送者的 IP 地址，来过滤邮件。在过滤设置里操作。

过滤	描述
允许的 IP 区间	加入任何你希望加入到你白名单的 IP 地址或者网络。如要加入一个单独 IP 地址，使用子网掩码 255.255.255.255。列入白名单的 IP 地址绕过垃圾邮件评分及其他的黑名单但是附件、信体及主题将进行过滤在加入行后，点击加入，再保存修改。
阻断的 IP 区间	加入你希望加入到黑名单的任何 IP 地址或者网络。加入一个单独的 IP 地址，使用子网掩码 255.255.255.255。列入黑名单的 IP 地址/网络绕过所有白名单，除去基于 IP 地址/网络的白名单。你可以指定是否 IP/区间应该被阻断，隔离或者标记。在加入行后，点击加入，再保存修改。

5. 发送者的域过滤

在过滤设置里，发件人域黑白名单允许你根据发件人的邮件地址来过滤邮件。

过滤	描述
允许的 发件人 域/子 域	加入任何你希望记入到白名单的域或者子域。 将一个域加入到白名单，自动将所有子域加入到白名单。 举例，将 customer.com 加入，允许 joe@customer.com 及 joe@office1.customer.com 的邮件。将域/子域加入白名单绕过垃圾邮件评分及其他黑名单，除去 IP 阻断/接受及信体/主题过滤加入行后，点击加入，再保存修改。 <i>不要使用通配符，比如*或@，只要输入域名就可以了。</i>
阻断 发件 人域/ 子域	加入任何你希望阻断的域或者子域。 阻断一个域，自动阻断所有子域。 如，加入 spammer.com 阻断所有 joe@spammer.com 及 joe@server1.spammer.com 的邮件。将域/子域加入黑名单绕过所有白名单，除去基于 IP 地址/网络及域/子域的白名单。你可以指定是否 IP/区间应该被阻断、隔离或者标记。加入行后，点击加入，再保存修改。

6. 发送者邮件地址过滤

基于发件人的地址来过滤邮件。

过滤	描述
允许的邮 件地址	将你希望的发件人邮件地址加入到白名单加入后点击加入，再保存修改。
阻断的邮 件地址	将你希望的发件人邮件地址加入到黑名单，指定该发件人是应该被阻断、隔离还是标记加入后点击加入，再保存修改。

7. 接受者邮件地址过滤

根据邮件的接受者来过滤邮件。

过滤	描述
允许的邮 件地 址	将你希望的收件人邮件地址加入到白名单。加入到白名单的收件人的邮件将不再进行垃圾邮件评分加入白名单的收件人绕过垃圾邮件评分及其他黑名单，除去 IP 阻断/接受及信息/主题过滤。加入后点击加入，再保存修改。

阻断的邮件地址	将你希望的收件人邮件地址加入到黑名单，指定是否该收件人的邮件应该被阻断、隔离还是标记。一个常见的阻断一个收件人地址邮件的原因是该用户不再是你公司成员，但是你希望在邮件服务器上保存帐号。加入到黑名单的收件人再也收不到邮件，除非设置了接受发件人 IP 地址、域、邮件地址的过滤。加入后点击加入，再保存修改。
---------	---

注意：在加入白名单或黑名单时，请填写备注，以便标识各个不同的记录。

8. 附件过滤

在过滤设置里，可以设置基于邮件的附件来过滤病毒或垃圾邮件。附件过滤根据它包含的文件扩展名来允许你阻断或隔离邮件。

梭子鱼垃圾邮件防火墙允许的最大默认附件大小是 100 兆字节。如果邮件超过了这个大小，梭子鱼将拒绝此份邮件，并且发送服务器将通知发件人此邮件未发送到目的接受者。

所有邮件，包括哪些列入白名单的发件人，都将经过附件过滤。这意味着，如果一个发件人在你的白名单上，发了一个带有不允许的附件类型的邮件，该邮件将被阻断或者隔离（根据你的设置）。

过滤	描述
附件阻断	
阻断的件的扩展名	添加想阻断的文件扩展名（不要加.），如果一份邮件包含其中一个扩展名的文件，那么此邮件会被梭子鱼阻断。
阻断压缩文件夹中包含以上扩展名的文件	如选择“是”，将会对文件夹中的内容进行扫描并阻断包含你加入的扩展名的文件。如果文件中包含这些扩展名的其中之一，那么梭子鱼将阻断这份邮件。
阻断被密码保护的文件	选择“是”，系统将阻断包含被密码保护文件的邮件。（比如 zip 文件）被密码保护的文件不能进行扩展名的扫描。由于这个原因，你可能想阻断此类型的文件。
阻断通知	
通知收件人被拦截的文件	选择“是”，系统在阻断包含以上被禁止的扩展名文件的进入邮件时，会通知收件人。
通知发件人被拦截的文件	选择“是”，系统在阻断包含以上被禁止的扩展名文件的进入邮件时，会通知发件人。
附件隔离	
隔离附件的扩展名	添加要隔离附件的扩展名（不要写“。”）。梭子鱼会将包含这类附件的邮件发送到隔离信箱。
隔离压缩文件中包含上述扩展名的文件	选择“是”，系统会对压缩文件（比如 zip 文件）进行扫描你想隔离的文件扩展名。梭子鱼会隔离压缩文件中含有此类扩展名的邮件。
隔离密码保护的文件	选择“是”，系统将会隔离包含密码保护文件（如 zip 文件）的邮件。被密码保护的文件不能进行扩展名的扫描。由于这个原因，你可能想阻断此类型的文件。

9. 主题过滤

主题过滤可以允许你基于邮件的主题行来过滤邮件。修改后请保存。

邮件主题阻断	输入单词，常用语，字符等，如果他们在邮件的主题行中出现，那么此份邮件将被阻断。
邮件主题隔离	输入单词，常用语，字符等，如果他们在邮件的主题行中出现，那么此份邮件将被隔离。
邮件主题标记（接收过滤模式）	输入单词，常用语，字符等，如果他们在邮件的主题行中出现，那么此份邮件将被标记。
邮件主题白名单	输入单词，常用语，字符等，如果他们在邮件的主题行中出现，那么此份邮件将被列入白名单。

注意：

- 你可以输入多行过滤内容，但是每行只能包含一个单词或常用语。每行是独立应用的。
- 在 HTML 源代码中字符之间嵌入的 `html` 注释和标记也会被过滤，这样 web 浏览器中出现的实际的单词都会被过滤掉。

10. 信体过滤

信体过滤可以基于邮件正文的内容来过滤邮件。修改后请保存。

邮件内容阻断	输入单词，常用语或字符，如果他们出现在邮件正文中，那么此邮件将会被阻断。
邮件内容隔离	输入单词，常用语或字符，如果他们出现在邮件正文中，那么此邮件将会被隔离。
邮件内容标记（接收过滤模式）	输入单词，常用语或字符，如果他们出现在邮件正文中，那么此邮件将会被标记。
邮件内容白名单	输入单词，常用语或字符，如果他们出现在邮件正文中，那么此邮件将会列入白名单。



11. 信头过滤

信头阻断	输入单词，常用语或字符，如果他们出现在邮件信头中，那么此邮件将会被阻断。
信头隔离	输入单词，常用语或字符，如果他们出现在邮件信头中，那么此邮件将会被隔离。
信头标记（接收过滤模式）	输入单词，常用语或字符，如果他们出现在邮件信头中，那么此邮件将会被标记。
信头白名单	输入单词，常用语或字符，如果他们出现在邮件信头中，那么此邮件将会被列入白名单。

八、 用户设置和域设置

1. 梭子鱼垃圾邮件防火墙如何创建用户

梭子鱼在满足以下情况会自动创建一个新的用户：

-  隔离类型设置为“分用户”。
-  梭子鱼接受到一份需要被隔离的邮件。

梭子鱼系统会采取以下动作：

1. 在数据库中检查接受者邮件地址
为了提高安全性，你可以将梭子鱼配置为在建立新帐户之前要对邮件接受者进行验证（使用 LDAP 或 SMTP）。这可以阻止梭子鱼为无效用户建立帐户。
2. 如果这个地址不存在，系统会为它建立一个新的用户。（梭子鱼使用接受者的邮件地址作为帐户名且自动生成密码）
3. 将登录信息发送给用户，这样他们就可以访问隔离信箱。
4. 将隔离信放到接受者的隔离信箱中
5. 向用户发送隔离通知
 因为梭子鱼会自动建立帐户，所以你不需要手动添加新帐户。

2. 查看用户帐户

在用户设置—》账号管理页面显示了梭子鱼系统上所有的用户帐户。你可以完成以下任务（下面表格中的功能内容，根据型号不同会有些功能处于不可见状态）：

- 编辑用户帐户的设置
- 删除用户帐户
- 改变任意一个指定的帐户的密码

帐户地址	帐户的邮件地址
通知间隔	系统向用户发送隔离通知的频率
隔离	用户是否使用隔离帐户。如果此项设置为“否”，所有的隔离邮件都会直接发送到用户信箱中，而不会发送到用户的隔离信箱中。
使用垃圾邮件扫描	是否启用垃圾邮件扫描。如果设置为“否”，那么这个用户的邮件不会被进行垃圾邮件扫描。
大小 (KB)	当前用户隔离区的大小。可以知道用户占用磁盘空间的大小。
隔离邮件数	当前用户隔离区的邮件数量。
最早的隔离邮件	在用户隔离区的最早的邮件。
管理员动作	<p>点击“编辑帐户”可以改变帐户的界面和垃圾邮件评分值。</p> <p>点击“更改密码”可以改变帐户的密码</p> <p>点击“删除”，将会从系统上把此隔离帐户删除包括被隔离的邮件</p>
删除所有无效账号	这个按钮将会清除所有无效用户的帐户。

3. 使用过滤条件来查看帐户

你可以使用下面描述的条件来查看帐户。

帐户 (邮件地址)	只显示此邮件地址的帐户
帐户 (类型*)	<p>显示符合全部或部分类型文本栏里输入的用户名的帐户。这个匹配应用到梭子鱼上存在的所有域。</p> <p>注意：通配符应用到类型的右边。这意味着如果你查找bob的话，那么 bob@domain.com 和bobby@domain.com都将匹配，但是billybob@domain.com不匹配。</p>
帐户 (*类型)	<p>显示符合全部或部分类型文本栏里输入的用户名的帐户。这个匹配应用到梭子鱼上存在的所有域。</p> <p>注意：通配符应用到类型的左边。这意味着如果你查找domain.com的话，那么 user@domain.com 和user@corp.domain.com都将匹配，但是user@domain1.com不匹配。</p>
启用隔离	显示所有启用隔离的帐户
禁用隔离	显示所有被启用隔离的帐户
启用垃圾邮件扫描	显示所有启用垃圾邮件扫描的帐户
禁用垃圾	显示所有未启用垃圾邮件扫描的帐户

邮件扫描	
------	--

4. 编辑用户帐户

在以下情况下，你可能需要编辑指定用户的帐户设置：

- 在用户的隔离信箱中检查邮件
- 修改用户的隔离设置和垃圾邮件设置
- 添加邮件地址到用户的白名单或黑名单（解决用户不能收到正常邮件或用户收到了大量的垃圾邮件）

修改用户的帐户：

1. 进入用户设置—》帐户管理
2. 在管理员动作这列，点击你想修改的帐户旁边的“编辑帐户”。出现一个新的此帐户页面
3. 在隔离邮件箱和选项这两个页面里做相关的修改

5. 删除无效的用户帐户

在用户设置—》帐户管理页面，你可以删除不存在于你邮件服务器或 LDAP 服务器（如果被启用此认证）上的无效帐户。

你可以点击按钮“删除所有无效帐户”。出现一个状态页面显示了删除帐户的统计信息。

在删除无效帐户之前，请注意：

- ✚ 删除无效帐户可能会持续很长时间。系统需要 1 至 2 秒来验证帐户，大约 3 至 5 秒来删除无效帐户。
- ✚ 如果想停止删除过程，点击状态统计页面上的“停止”按钮。
- ✚ 如果你关闭 web 管理接口，也不会中断删除无效帐户的此进程。
- ✚ 删除无效帐户的同时，也会删除无效帐户隔离信箱中的邮件。

6. 为帐户指定相关选项设置

在用户设置—》用户选项页面，你可以指定用户界面的选项

隔离功能	<p>决定你的用户是否启用隔离信箱。如果你设置为“否”，那么在以下情况下邮件将会被隔离：</p> <ul style="list-style-type: none"> ■ 在基本设置—》隔离设置页面来设置 ■ 在域设置—》选择你需要编辑的域
垃圾邮	决定了用户是否启用此功能

件扫描功能	
可修改通知时间	决定了用户是否可以改变接受隔离通知的时间。如果你设置为“否”，所有的用户都会基于你在基本设置—》隔离页面设置的时间接受到隔离通知。如果设置为“是”，那么用户可以自己改变接受隔离通知的时间。
黑白名单	决定了用户是否可以将邮件地址或域加入到他们的个人黑白名单中。
使用贝叶斯	决定了用户是否可以查看和编辑他们的贝叶斯数据库。
可修改评分	决定了用户是否可以修改阻断，隔离，标记的分数等级。如果你设置为“否”，那么垃圾邮件评分都是基于： <ul style="list-style-type: none"> ■ 基本设置—》垃圾邮件评分页面里的设置。 ■ 域设置—》选择一个域，在这里设置的垃圾邮件评分规则。
自定义用户选项	你可以为一个用户指定不同的选项。在用户帐户框内输入你想改变的帐户，指定相关选项后请保存。

7. 添加或更新用户帐户的隔离设置

你不需要建立新帐户，因为梭子鱼在启用分用户隔离功能后会自动建立帐户。如果你想改变一个用户的设置，你可以在这里修改。

例如：

常见重要的隔离设置情况是你想为一部分用户在梭子鱼上建立隔离信箱，而让其余的用户在他们自己的邮箱中接受隔离邮件。你可以让拥有隔离信箱的用户完全控制并管理他们的隔离邮件队列。只为一部分重要的用户提供隔离信箱。

在这个例子中，你可以这样设置：

- 设置隔离类型为分用户隔离
- 将默认隔离设置关闭，这样用户在梭子鱼上就没有隔离信箱了。
- 输入你想为他们建立隔离信箱的用户的邮件地址，并将“启用用户隔离”设置为“是”。

Override? 为指定的用户修改隔离设置：

1. 在用户帐户框内输入你想改变的用户的邮件地址，每行一个邮件地址。
2. 选择你列出的这些用户是否启用隔离功能。
3. 选择是否是新建的用户。
4. 点击保存。

8. 设置邮件策略

邮件在梭子鱼上的保留策略能自动管理用户的隔离信箱。

你可以通过以下两种方式来控制隔离信箱的大小：

- 隔离区大小限制—决定了每个用户隔离区的大小
- 邮件有效期限限制—决定了在用户隔离区中保留的邮件的期限

建议你让用户自己管理他们自己的隔离信箱，而不要依赖于邮件策略，因为这样会影响梭子鱼系统的性能。

另外，你可以在用户设置—》帐户管理页面看到每个帐户的隔离区的大小。这样如果一个用户的隔离区非常大，你可以直接告诉他去清理一下。

注意：邮件策略的执行时间在 02:30 AM。

9. 管理你的隔离信箱

从梭子鱼接受到的两种类型的邮件：

- 通知邮件
- 隔离通知报告

通知邮件：

梭子鱼第一次隔离你的一份邮件时，系统会发送一个主题行为“用户隔离帐户信息”的通知邮件。通知邮件包含以下信息：

欢迎访问梭子鱼垃圾邮件防火墙。这份邮件包含你访问隔离信箱的相关信息。你的帐户是：

用户名：《你的邮件地址》

密码：《你的默认密码》

使用以下链接直接访问你的隔离信箱：

<http://<梭子鱼系统的地址或名称>:8000>

梭子鱼会自动建立你登录信息（用户名和密码）和登录隔离信箱的链接。你应该保留此份邮件，以后系统不会再发送你的登录信息给你。

隔离通知：

梭子鱼每天都会发送一份隔离通知给你，你可以看到自己被隔离的邮件。你可以把邮件发送到你客户端信箱中，添加到白名单，或删除此份邮件。

下图是一个隔离通知图示：



登录到隔离信箱：

1. 点击上图隔离通知下方的链接，就出现登录界面
2. 输入你的用户名和密码，点击登录。（你的登录信息在发给你的通知邮件中）

管理你的隔离信箱：

在登录到隔离信箱后，可以看到所有你被隔离的邮件。当你第一次登录的时候，你应该尽可能多的分类邮件。

梭子鱼有一个学习引擎，它会基于你对邮件的分类来处理将来的邮件。随着你分类邮件的时间的推移和你加入的黑白名单的规则，这个学习引擎会更有效率。

选择一份邮件后，你可以执行以下动作：

发送	发送被选择的邮件到你的信箱中。如果梭子鱼发送一份邮件的话，就不会保存在这个隔离信箱中了。
白名单	将此邮件的发件人加入到白名单中，以后此人发送的邮件只有在包含病毒或被禁止的附件时才会被隔离。
删除	把选择的邮件删除，删除后的邮件不能被恢复。
分类为垃圾邮件	将选择的邮件分类为垃圾邮件
分类为正常邮件	将选择的邮件分类为正常邮件（更有效的方式是加入到黑白名单）

改变你的帐户密码：

- ◆ 在隔离信箱登录界面点击创建新的密码 或
- ◆ 登录隔离信箱后进入选项页面，输入旧的密码，新密码后，点击保存密码。如果通过 LDAP 或 Radius 启用单点登录的话，那么此选项不可用。

注意：改变密码后，你会收到一个新的隔离通知，包括新帐户的信息。

改变你的隔离设置：

你可以按照以下描述来改变设置。

选项一》隔离设置页面

启用隔离	决定梭子鱼是否隔离你的邮件。设置“是”，梭子鱼不会发送隔离邮件到你的客户端邮箱，但是你可以通过隔离信箱和隔离通知来查看这些邮件。 设置为“否”，梭子鱼把所有被隔离的邮件以主题行[quar]（管理员可以修改此前缀）发送到你的客户端邮箱中。
通知间隔	梭子鱼发送隔离通知的频率。如果你设置为“从不”，那么你从来都不会收到隔离通知，但是你可以在隔离信箱中看到被隔离的邮件。
通知地址	梭子鱼发送隔离通知的目的地址。
默认语言	指定隔离通知的语言。所有从梭子鱼发出的隔离通知是 UTF8 的编码。它不会影响到其他用户。

启用或禁用垃圾邮件扫描功能：

如果你不想让梭子鱼扫描你邮件的内容，你可以在选项一》过滤设置页面关闭垃圾邮件的过滤功能。同时可以改变标记，隔离或阻断邮件的默认评分设置。当梭子鱼接受到发给你的一份邮件时，它会对此邮件进行评分。这个分数的范围是从 0（正常邮件）到 10（垃圾邮件）或更高。如果设置为 10，表示关闭此功能。

垃圾邮件扫	
-------	--

描功能	
启用垃圾邮件扫描	选择“是”，梭子鱼会对你的邮件进行扫描。 选择“否”，梭子鱼不会对邮件进行垃圾邮件扫描。
评分设置	
使用系统缺省设置	选择“是”，使用系统默认的评分设置。选择“否”，在下面写入你期望的评分数值。
标记分值	高于此分和低于隔离分的邮件的主题行都会添加一个单词 (bulk)。任何低于此分的邮件都是允许的。默认数值是 3.5
隔离分值	高于此分和低于阻断分的邮件的主题行都会被发送到你的隔离信箱中。默认数值是 10 (禁用隔离)。这个分值必须小于阻断分值，才能使用此功能。
阻断分值	高于此分值的邮件都不会发送到你的客户端邮箱中。默认分值是 9
梭子鱼贝叶斯学习	
重新初始化贝叶斯数据库	点击“重新初始化”按钮，将会删除梭子鱼从安装时学习的贝叶斯规则。
梭子鱼贝叶斯备份	点击“备份”按钮，会把数据下载到本地桌面上。
恢复数据库	点击“浏览”按钮，选择你以前所做的备份文件后，点击“上传”，就会把贝叶斯数据上传到梭子鱼防火墙上。

将邮件地址或域添加到你的黑白名单中：

在选项页面一》黑白名单页面里添加

白名单	添加你希望接受邮件的地址或域。梭子鱼会由于病毒或不允许的附件而阻断这些人发给你的邮件。
黑名单	加入你不想接受邮件的地址。梭子鱼会立即抛弃从这些人发送来的邮件。发送者和你都不会收到此邮件被删除的通知。

按以下步骤添加黑白名单：

1. 选择选项一》黑白名单

这里列出了已有的黑白名单地址

2. 如需删除一条记录，请点击旁边的删除按钮
3. 如添加一条记录，在方框中输入地址，点击“加入”。

注意：

- 如果你输入一个完整的地址，那么只指定这个用户。如果你输入一个域，如 yahoo.com，那么此域中的所有用户都被指定了。
- 如果你输入一个域，如 yahoo.com 那么它所有的子域也被包括了，如 mail.yahoo.com。
- 你应该把邮件的“from”地址加入到黑白名单中

改变登录隔离信箱的语言：


你可以改变你的隔离信箱的语言，在隔离信箱一》选项页面右上角的下拉列表。支持的语言有中文，日文，西班牙语，法语等等。


你选择的语言不会影响到其他用户。

10. 添加新域

首次安装时，需要添加允许梭子鱼接受的域。基本设置包括目的邮件服务器和你的域名。

在梭子鱼上有两种添加域的方法：

 从基本设置—》IP 设置，在页面的下方加入“允许的接受域”。

 从域设置页面添加域名。

如果你的梭子鱼需要过滤几个邮件服务器或域的话，你需要在域设置页面添加相关的邮件服务器。

如果你的梭子鱼型号是 400，600 或是 800 的话，你可以基于每个域来设置垃圾邮件评分，隔离类型和垃圾邮件与病毒检查。

添加或编辑域：

1. 选择域设置页面
2. 在高级域名设置下面的方框中输入相关的域后，点击添加域名。这样新域就出现在列表中了。
3. 选择此域，点击编辑域。一个域编辑页面出现了。
4. 配置相关设置，*参考下面编辑域设置*。

11. 编辑域

1. 在域设置页面选择你想编辑的域，新的编辑域的页面出现了。
2. 指定下表描述的分域设置。**这些设置只适用于梭子鱼 400 型号或以上。**
3. 填写好请保存。

目标邮件服务器和目标端口	填写你选择的域的邮件服务器的地址或名称和端口。
使用MX记录	是否对目标邮件服务器进行MX查询
有效的测试邮件地址	输入一个有效的邮件地址来测试梭子鱼是否能过滤此域的邮件。可以点击“测试SMTP连接”按钮来测试。确定测试邮件地址接受到此测试邮件。
Realm名	Realm是一个可以验证有效用户名和密码的数据库
标记，隔离，阻断分值	可以设置基于此域的垃圾邮件评分标准，不会影响其他域。这里的设置将会优先于在基本设置—》垃圾邮件评分设置的标准，但是用户登录到隔离信箱设置自己的垃圾邮件评分标准会优先于域设置。
分用户隔离	决定此域的隔离类型。 <i>请参考指定隔离类型</i>
全局隔离邮件地址	指定此域的全局隔离邮件的接受地址。
垃圾邮件和病毒扫描	决定此域是否启用垃圾邮件或病毒扫描。

欺骗防护	梭子鱼是否阻断使用你的域作为“from”地址的外发邮件。如果设置为“是”，梭子鱼会阻断 from 地址是“梭子鱼允许接受的域”的所有邮件。
------	---

12. 设置 LDAP

使用 LDAP 对邮件的接受者进行验证，以阻止虚假的接受者。

配置 LDAP:

1. 选择域设置页面
2. 点击你想设置认证的那个域后面的“编辑 LDAP”。
3. 在出现的页面里填写所需的相关信息。

LDAP 服务器	你对接受者进行认证的 LDAP 服务器的地址。如果为了安全目的，你可以指定两个 LDAP 服务器，他们之间用空格分开。同时两个 ldap 服务器的用户名，密码，过滤器，search base 和端口必须是相同的。
LDAP 端口	是梭子鱼与 LDAP 服务器通信使用的端口。默认是 389。
Exchange 加速器启用	决定了是否执行邮件接受者的 LDAP 查询认证。选择“是”，那么梭子鱼会使用 LDAP 的设置。选择“否”，梭子鱼会默认通过 rcpt to 命令进行 SMTP 认证，默认使用这种 SMTP 认证时，如果服务器返回代码不兼容或梭子鱼无法识别，将会造成认证失效，产生虚假发件人的情况。
统一邮件别名	梭子鱼为单个的用户统一所有的邮件别名。选择“是”，梭子鱼会将发送到任何一个用户别名的邮件发送到同一个隔离信箱中。梭子鱼 200 型号不支持此功能。统一别名的特征把个人的别名链接在一起。如：如果 sanderson@acme.com,sandy_anderson@acme.com 和 sanderso@acme.com 属于同一个帐户，那么梭子鱼会将这些别名链接到主帐户。
SSL/TLS 模式	LDAP 支持两种安全传输模式： LDAPS:LDAP 协议版本 2 最初使用的模式。在 SSL/TLS 初次协商时使用的是典型的带外连接，而在连接后使用此 SSL/TLS 通道。LDAPS 端口通常是 636。 StartTLS: LDAP 协议版本 3 使用的。此模式在初始建立的时候是不安全的。客户端会告诉服务器它希望切换到 SSL/TLS 模式。如果服务器支持 StartTLS，那么 SSL/TLS 就会建立，以后的通信就会安全了。StartTls 与明文认证使用的端口是兼容的，默认是 389。 如果关闭 SSL/TLS，那么梭子鱼与 LDAP 的通信是以明文进行的。如果你梭子鱼和你的 LDAP 服务器属于同一个私网或使用匿名认证(意思是不需要用户名和密码)，那么使用明文认证是可以的。明文认证比通过 SSL/TLS 认证更有效率，因为 SSL/TLS 认证会产生延迟，尤其是与 LDAP 服务器连接的时候。
Require TLS/SSL	如果启用此功能的话，发送和接受方的系统(需支持 TLS/SSL)都会以密文来发送密码。如果其中一方不支持 TLS/SSL,那么系统间的流量是不被加密的或不安全的。
Bind DN	LDAP Exchange 服务器的用户名。确定完全合格的用户名，打开活动目录，进入活动目录用户及电脑，双击有问题的用户帐户。在帐户标签下，使用用户登录名加@xxx.xxx 做为 LDAP 用户名。

Bind Password	LDAP Exchange 服务器的密码
LDAP 过滤器	自定义应用到此域的 LDAP 过滤器
LDAP search base	在 LDAP 目录树中起始搜索点。默认的查询值是“defaultNamingContext”。如果在一个林中你有两个域，并且对于两个域你想使用同一个 LDAP 服务器来做认证，请将 search base 设置为 DC=com，端口是 3268。这会允许在 .com 域和全局目录下进行完全的查询。
LDAP UID	LDAP 过滤器使用的容器。梭子鱼通过此过滤器来认证梭子鱼上的用户帐号。主要用于统一别名和单点登录。默认是 uid，最近的活动目录设置为 sAMAccountName。
LDAP Primary Email Alias	当统一邮件别名功能启用的时候，这个属性为所有基于此别名的邮件接受者提供了存储隔离邮件的帐户。对使用 LDAP 的单点登录来说，这个是他们使用别名直接登录的用户名。这个属性是 mail，应该是一个有 @ 连接的域的完全合法的地址。这个域是在梭子鱼上配置的有效域。
Canary email	在梭子鱼正常工作的时候，这个地址决定了是否对这个域进行了 LDAP 的有效性认证。如果此项为空的话，在认证失败期间 LDAP 接受者认证和统一邮件别名将被禁用。
有效的邮件地址（测试用）	这个邮件地址是用来做测试用的。（点击测试 LDAP）测试是为了确定上面所做的设置的正确性，包括 LDAP 地址，UID 和 LDAP primary Email Alias 等。

LDAP 服务器出现故障带来的影响：

如果你的 LDAP 服务器由于不确定的原因 down 机了，那么梭子鱼就不会对邮件接受者进行认证了。在 LDAP 服务器恢复之前，梭子鱼会为接受了邮件的接受者建立帐户。一旦 LDAP 服务器恢复了，请删除任何无效帐户。（参考添加或更新指定的用户的隔离设置）。

如果你使用统一邮件别名，梭子鱼会由于找不到主名称而返回一个 421 的重试邮件到发送者的邮件服务器。这可以避免建立相同的帐户。

标准邮件服务器的常用设置：

下表提供了邮件服务器常用的 LDAP 用户名，LDAP 过滤器和 Search base。

Micro soft exchange 5.x	LDAP Bind DN: cn=<用户名>, dc=<域>, cn=admin 如：cn=username,cn=users,dc=domain,dc=com 域应该是 NT 域名而不是邮件的域名（除非他们是相同的）。为了验证掩藏的接受者，admin 的后缀是必须的。 LDAP 过滤器和 Search base 保留默认设置。
Micro soft exchange 2003	常 用 的 过 滤 器 是 : ((proxyaddresses=smtp:\${recipient_email}))(mail=\${recipient_email}))
一个接受域的 Lotus Domin	LDAP Bind DN: username@domain.com LDAP 过滤器: ((mail=\${recipient_email})(cn=\${recipient_local_part})(shortname=\${recipient_local_part})(fullname=\${recipient_local_part}))

o	
两个接受域的 Lotus Domino o	如果你 lotus Domino 服务器有两个接受域，但是你每个用户只有一个单独的互联网地址，请使用下面的过滤器来认证两个域： <code>((mail=\${recipient_email})(cn=\${recipient_email})(uid=\${recipient_email}))</code> 如： username@abc.com 可以接受发地址为username@abc.com或username@xyz.com的邮件且对username@abc.com进行LDAP认证， 但是不能对username@xyz.com认证 。使用此过滤器就可以对两个域进行LDAP认证。
Novell group wise	LDAP Bind DN: cn=username,o=organization 过滤器和 search base 保留默认。

九、高级设置

1 邮件协议

在高级设置一》邮件协议里可以改变 SMTP 检查的默认设置。下表描述了此页面的每个选项。修改后，请保存。

需要 SMTP helo	决定连接梭子鱼的客户端是否需要发送 smtp helo 命令，选择“是”，会阻止非法用户利用垃圾邮件发送程序来自动发送邮件。默认设置为“否”。
邮件须符合 RFC821 规范	梭子鱼是否需要 SMTP “MAIL FROM”和“RCPT TO”命令包含以’<’和’>’封装的邮件地址。同时 SMTP “MAIL FROM”和“RCPT TO”命令中也不能包含 RFC822 类型的短语或注释。设置为“是”，不仅会阻止从垃圾邮件发送者也会阻止不使用 RFC821 标准的 windows 邮件客户端程序发来的邮件（如微软的 outlook）。由于这个原因，默认设置是”否“。
需要完全合法的发件人域名	决定梭子鱼是否需要完全合法的域名
拒绝虚假发件人域名	决定了梭子鱼是否拒绝在 DNS Server 中没有 MX 记录的邮件。
发件人欺骗防护（spoof）（仅接收过滤模式）	梭子鱼是否阻止此域作为”from”地址的外发邮件。 选“是”，它会阻止 from 地址是梭子鱼接受邮件域的外发邮件。 如果你域内所有的邮件直接发送到邮件服务器不经过梭子鱼，那请你启用此功能。
发送者策略框架（SPF）/微软 Caller ID 框架	SPF 和微软 SenderID 框架可以帮助梭子鱼区分非法用户和合法用户。启用此选项，将会由于 DNS 的查询（查找域的 SPF 或 SenderID 记录）而影响系统性能。默认设置是“否”。
可信任的发送主机 IP	这个列表里包含了任何你允许的外部主机转发邮件到梭子鱼上的 IP 地址。当执行 SPF/SenderID 检查时，会忽略此列表中的地址。
SMTP 收件超时	设置接受邮件需要的时间限制。默认是 30 秒。设置 smtp 传输的时间限制会阻止非法发送者与梭子鱼维持长时间的连接而影响系统性能。超过此限

	制的邮件被阻断，在邮件日志中看到原因是超时。如果在日志中看到有大量此种原因阻断，请适当设置延长此时间。
每个 SMTP 会话的邮件数量	对每个 SMTP 会话的邮件数量的限制。如果一个会话中邮件数量超过这个限制，那么其他的邮件在邮件日志中就会被阻断，原因是“超过了每连接邮件数的限制”。
SMTP 欢迎横幅	连接到梭子鱼的客户端是否收到欢迎横幅
去除梭子鱼信头	在邮件从系统发送出去后删除梭子鱼定义的信头。推荐你不要删除梭子鱼的信头，因为他们包含了邮件被标记，隔离或隔离的原因。降低了排除故障的难度。

2 速率控制

速率控制可以让你配置在半小时内从同一个 IP 地址发起建立的连接数。速率控制可以防止非法用户或垃圾邮件程序在很短的时间内发送大量的邮件到你系统上。

邮件速率控制	指定在半小时内同一个 IP 地址允许的最大连接数。这个设置只有在多于五个独立 IP 地址连接时有效。当连接数超过速率限制的极限时，梭子鱼会阻断以后的连接或邮件。合法的发送邮件服务器会告诉发送者重试一次。
排除速率控制的 IP 区间	指定你希望速率控制排除的 IP 地址区间。输入单个的 IP 地址，请写掩码 255.255.255.255。

3 限定用户

激活单独的帐户。当你首次安装梭子鱼时，你可能只想过滤一些用户。在熟悉了解梭子鱼系统后，你可以应用到所有用户。



下面是激活用户的步骤：

1. 选择高级设置—》限定用户
2. 在地址栏中输入要激活的帐户的邮件地址
3. 点击添加

注意：只有列表中添加的邮件地址会被梭子鱼进行垃圾邮件扫描和病毒的保护。但是，**RBLs,速率控制和接受者验证**则适用于所有进入的邮件。

4 配置备份

如果你想把你的系统配置导入到一个替代产品上或是你当前系统数据出现错误，那么你应该先备份你的系统配置。在高级设置—》配置备份页面，有两种备份类型：

-  桌面备份—将备份文件保存到你的本地桌面
-  自动备份（推荐）—按照你的计划自动备份

以下信息不包括在桌面或自动备份文件中：

- ◇ 系统密码
- ◇ 系统 IP 信息
- ◇ DNS 信息

注意：不要编辑备份文件。你需要改变的任何配置请通过 web 管理界面来更改。备份文件包含了一个校验码，如果这个校验码被改变，文件就不能被上传到系统上。

桌面备份：

1. 在高级设置—》配置备份页面，选择你想备份的文件：

系统配置文件	所有全局和系统设置（不包括系统密码，系统 IP，和 DNS 信息）
用户设置	所有除了贝叶斯数据库之外的用户设置
贝叶斯数据	所有全局贝叶斯数据

2. 点击备份按钮，保存备份文件到本地系统。

自动备份：

到梭子鱼系统的高级设置—》配置备份页面，填写完以下所需的信息：

服务器类型	保存备份文件的服务器类型（包括 FTP 或 SMB）。选择你使用的自动备份服务器类型。选择“off”，就不再自动备份。
服务器名称/IP	备份服务器的地址或合法的名称
用户名	梭子鱼防火墙登录备份服务器的用户名
密码	梭子鱼用来登录备份服务器的密码
端口	FTP 或 SMB 服务器使用的端口
文件路径	在备份服务器上保存备份文件的文件夹，路径或共享名。
测试备份服务器	在使用自动备份之前，我们推荐你点击“测试备份服务器”来测试一下相关的设置。
备份计划	这里列出了你想备份的组件和每个备份的计划时间。选择好备份组件后，请指定备份的频率（每天或每周）
备份数目	At one time 保存在备份服务器上的备份数目。当超过这个数后，最早的备份文件会被删除。

恢复系统配置：

1. 到高级设置—》配置备份页面
2. 恢复以下一种：
3. 如果你将配置导入到一个替代产品上，请升级：
病毒和垃圾邮件规则库（从高级设置—>规则库升级页面）
系统内核（从高级设置—>系统升级页面）

注意：你应该在下班后恢复系统配置。系统配置恢复时会花费几分钟时间，在这段时间内系统会停止服务。

规则库升级：

下表描述了规则库升级的相关信息：

当前版本	显示了梭子鱼系统上正在运行的系统版本
最新版本	显示可以用的最新的版本。如果梭子鱼运行的当前版本不是最新的，请点击“升级”按钮下载最新的版本。如果没有最新的版本，这个按钮是灰色的。
以前版本	显示系统以前安装的版本。想返回到这个版本，请点击“回复”按钮。
升级频率	决定了梭子鱼升级的频率。如果要关闭自动升级，选择“off”。 每天按梭子鱼系统的时间设置在上午 12:20 升级。
许可证	显示你的许可证状态。

病毒库升级：

当前版本	显示了梭子鱼系统上正在运行的系统版本，你可以点击“查看版本信息”来查看更多版本信息。
最新版本	显示可以用的最新的版本。如果梭子鱼运行的当前版本不是最新的，请点击“升级”按钮下载最新的版本。如果没有最新的版本，这个按钮是灰色的。
以前版本	显示系统以前安装的版本。想返回到这个版本，请点击“回复”按钮。
升级频率	决定了梭子鱼升级的频率。如果要关闭自动升级，选择“off”。 每天按梭子鱼系统的时间设置在上午 12:20 升级。
许可证	显示你的许可证状态。

系统升级：

在下载任何新的系统固件时，建议你完成以下任务：

- ✓ 把系统和用户设置备份
- ✓ 在下载之前，请阅读版本发布信息

应用新版本的系统内核时，系统服务会短暂的停止。所以，建议你在下班后应用新版本。

下载最新 **firmware** 版本:

1. 阅读版本发布信息
2. 点击立即下载（如果梭子鱼已经有最新版本的话，这个按钮将不可用）
3. 点击刷新按钮，查看下载状态。
4. 如果下载完成，你会看到“立即应用”按钮。你需要点击此按钮来应用已经下载的文件。
5. 点击立即应用后，系统会重启。不需要手动重启。几分钟后，你的系统就可以正常工作了。

5 外观设置

可以通过高级设置—》外观设置，来自定义管理界面的显示图片和发送到用户的隔离通知。这个功能是梭子鱼 400 型号以上产品才具备的。

通用外观	
梭子鱼 的名称	显示在登录界面上方（用户名和密码栏的上方）的梭子鱼系统的名称
Web 界面	
图片预览	显示将在管理界面使用的图片。在上传新图片到系统时，会出现。
上传新 图片	使用你自己的图片。点击浏览按钮，指定你想使用的图片后，点击“上传”。这里上传的图片会在管理界面的左上方显示，推荐的图片（jpg,gif,或 png）是 160×65 像素，小于 50k。
图片网 址	点击图片后指向的链接
重新设 置	把此设置恢复到默认设置。默认是博威特公司的标志。
隔离邮 件	
图片预览	显示将在管理界面使用的图片。在上传新图片到系统后，就会出现。
上传新 图片	使用你自己的图片。点击浏览按钮，指定你想使用的图片后，点击“上传”。这里上传的图片会在管理界面的左上方显示，推荐的图片（jpg,gif,或 png）是 480×66 像素，小于 100k。
标题背 景色	此颜色用于隔离邮件的表格头背景。
标题字 体色	此颜色用于隔离邮件的表格头字体。
重新设 置	删除自定义设置返回到默认的图片 and 颜色。

6 Syslog 日志

使用日志服务器对系统日志集中管理。

梭子鱼 200 型号产品不支持此日志功能。系统日志是发送系统日志的标准unix/linux工具，在所有unix/linux系统上都是可用的。有很多免费和优秀的厂商的日志服务器也适用于windows平台。博威特网络公司已经测试了很多免费日志服务器 (www.kiwisyslog.com)。

下面描述了你可以将两种不同类型的数据发送到日志服务器上。

邮件日志配置	写入你想接受邮件数据的日志服务器的地址。这些日志和邮件日志中使用的数据是一样的。点击“监控邮件日志”，将会出现一个查看邮件日志的新窗口。
Web 日志配置	<p>写入你想接受相关管理界面的日志服务器的地址。其中相关信息包括：</p> <ul style="list-style-type: none"> ✓ 用户登录 ✓ 用户什么时候从隔离信箱中删除或发送一份邮件 ✓ 梭子鱼配置的任何改变 ✓ 隔离通知产生的时间 <p>This syslog data appears on the local1 facility with login information at info priority, and configuration changes at debug priority.</p> <p>点击“监控 WEB 日志”，将会出现一个查看 WEB 日志的新窗口。</p>

7 信任转发

你可以通过 IP 区间，域或发送者来设置信任转发功能。**如果你想要通过梭子鱼外发邮件，请一定设置好此菜单。**

信任转发 IP 区间	输入梭子鱼信任转发的 IP 地址区间。如果你输入*通配符作为允许的邮件接受域，那么默认邮件服务器将可以使用梭子鱼来转发邮件。
信任转发主机/域	输入梭子鱼信任转发的主机或域名
允许转发的发送者	输入邮件地址或域名，这些用户将被允许在互联网上发送邮件给任何人。
信任转发	选择“是”，只允许上面指定的用户向外发送邮件。其它人都不能向外发送邮件。默认推荐是“否”
启用 SASL/SMTP 认证	<p>支持的认证有：</p> <ol style="list-style-type: none"> 1. None-关闭 SASL/SMTP 认证 2. LDAP-通过 LDAP 来进行认证 3. SMTP 认证代理-使用另一个 SMTP 邮件服务器来认证。因为梭子鱼是以明文形式传送密码的，所以建议配置加密方式：高级设置一》SMTP/TLS。

编辑 LDAP 设置	如果你使用 LDAP 认证，那么请输入你的 LDAP 服务器的相关信息。
SMTP 认证服务器	如果你使用 SMTP 认证方式，请输入认证服务器的地址。 用户提供的用户名和密码将通过 SMTP 认证命令转发给这台 SMTP 服务器。它可以是任何支持 SMTP 认证命令的服务器,比如微软的 Exchange 或者 Sendmail。

8 外发页脚

默认情况下，梭子鱼会在所有发送出去的邮件添加一个页脚。这个页脚会告诉邮件接受者此邮件已经被扫描了。

可以在高级设置—》外发页脚页面来改变默认的设置。

自动加上页脚	决定了外发邮件是否加上页脚
文本页脚	基于文本/ASCII 邮件的页脚
HTML 页脚	基于 HTML 邮件的页脚
页脚排除	列出了不会添加页脚的发送邮件地址。每行一个地址。

9 IP 高级配置

如果你的梭子鱼产品是 600 型号或以上的，你可以配置第二或第三个网络接口。

通过高级设置—》IP 高级设置，可以配置：

1. 输入相关网络接口的 IP 地址和掩码
2. 选择你将设置的相关网络接口
3. 点击“加入”，并保存
4. 重复以上步骤来设置其他网络接口

静态路由：

配置静态路由步骤：

1. 输入 IP/网络地址，网络掩码和网关地址
2. 点击“加入”，并保存

10 集群管理

你可以把多个梭子鱼系统链接在一起，这样他们可以同步系统配置。被集群的系统是不需要位于同一个网络的，它们可以是分散在不同地方的系统。

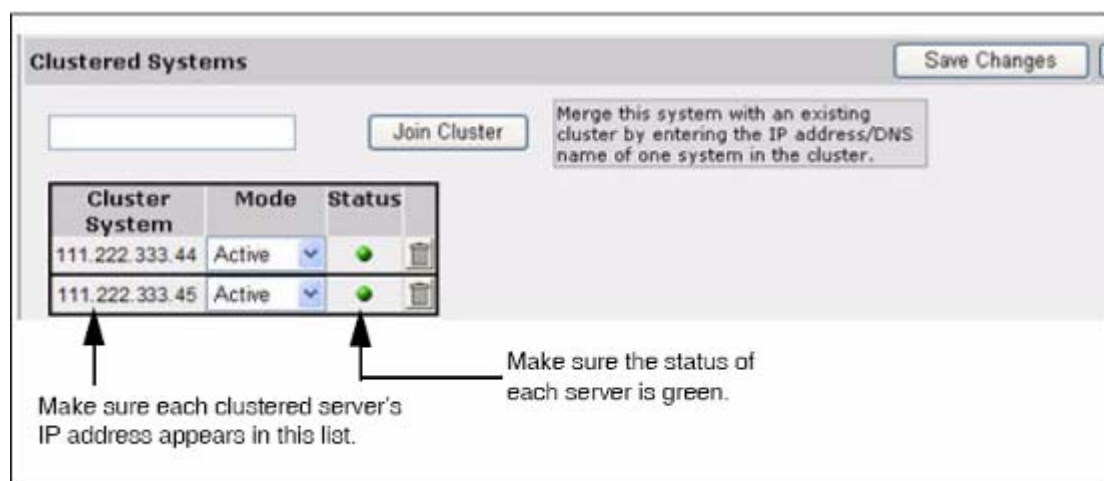
如果一个活动的系统出现故障了，你也可以在集群管理页面来指定使用备份系统。

梭子鱼 400 型号以上的系统才支持集群功能。

集群设置步骤：

1. 正确安装好要集群的每台设备
2. 到高级设置—》任务管理页面，确认没有其他进程正在运行。在两台设备上都要确认一下。
3. 在第一台设备上的高级设置—》集群管理页面，为集群输入一个共享的密码，保存一下。
4. 在第二台设备上的高级设置—》集群管理页面，按以下方式来做：
 - 1)输入相同的共享密码，保存
 - 2)在已集群系统旁的方框中输入第一台设备的地址，并点击“添加集群”按钮。
5. 在每台设备上，刷新一下集群管理的页面，确认以下：
 - 1)在集群系统的列表里的每个系统的 IP 地址
 - 2)每个系统的状态灯是绿色的

下图是一个示例：



6. 也可完成以下可选任务：
 - 把每台设备的 MX 记录的优先级设置为循环（至少需要其中一台设备处于活动状态）
 - 在你网络交换机上为两台集群设备配置负载均衡

集群管理页面的介绍：

下表描述了此页面相关项目的含义：

集群设置	
集群共享密钥	在集群中梭子鱼所共享的密码。集群中的梭子鱼必须使用相同的密码。在加入到集群之前，确保此密码已经被加入到此系统中。
集群主机	将要加入集群的系统的名称。集群中的其他系统将使用此主机名来连接此系

名	统。如果不写的话，那么将自动使用此系统的 IP 地址。如果 DNS 无法解析此主机名，你在加入到集群之前要在此页面的下方建立本地主机地图。
已集群系统	<p>你可以在此方框内输入将要加入到集群的梭子鱼系统 IP 地址和主机名，再点击“添加集群”。一旦系统加入到集群中，就会发生以下情况：</p> <ul style="list-style-type: none"> ● 集群中的系统配置将会覆盖此系统的设置。 ● 此系统上的用户列表会与集群同步，所以用户信息不会丢失。
集群系统列表	<p>在此列出了集群中的其他系统。模式指明了此系统是活动状态或备份状态。你可以指定一个备份系统。如果活动系统出现故障，那么集群就会使用此备份系统。</p> <p>只有活动的系统才能过滤进入的邮件。</p> <p>如果你想使用备份的系统来过滤邮件的话，你必须手动来把备份系统设置为活动状态。当活动系统出现故障时，不会自动切换到备份系统。</p> <p>状态灯显示了每个系统的状态（绿色—正在运行，红色—出现故障）</p>
本地主机视图	<p>为集群中的系统匹配主机名和 IP 地址。这个地图会忽略 DNS 的查找结果。这个地图不会和集群中的其他系统同步。</p> <p>在以下情况下使用本地主机地图： 集群的梭子鱼系统在不同的私有网络上。 不同的梭子鱼需转发到不同的邮件服务器上。在这种情况下，域管理界面里的目标邮件服务器可以是本地的邮件服务器。在本地主机地图区域里，集群中的每个梭子鱼会分配一个不同的 IP 地址给本地邮件服务器。</p>

集群设备间的数据传输：

配置集群不仅可以更方便管理多台梭子鱼设备，还能够为设备提供冗余。下表列出了当一个新系统加入到其他已集群的系统时传输的数据。

被传输的数据	不会被传输的数据
通过管理界面配置的系统设置（全局和域设置）	系统的 IP 地址
通过登录用户的隔离信箱做的分用户隔离设置	SSL 设置
邮件日志	
贝叶斯数据库	
隔离信箱	
用户帐户	

注意：新的系统只在它第一次加入到集群的时候，才传输它的贝叶斯数据库。已经完成集群设置后的系统间不会再同步他们的贝叶斯数据库。在以后的新版本中，将增加此功能。每个用户的帐户都使用集群系统中的主和备份设备。主设备是第一次加入到集群中的设备，备份设备是后来加入到集群的设备。两个设备任何时候都有相同的信息（配置和隔离邮件）。

改变已集群系统的 IP 的影响：

如果你的集群环境中的一个梭子鱼系统版本是 v3.1.x 或更早的，改变系统的 IP 地址就可以从集群将其删除。在你改变了其 IP 地址后，需要再次把系统添加到集群中。如果你的梭子鱼系统版本是 v3.2.x 或以上的，在你改变了系统的 IP 地址后，它还是集群中的一部分。

11 单点登陆

你可以配置梭子鱼使用 LDAP,POP,或 RADIUS 服务器来验证用户的帐户。这个功能在梭子鱼 400 型号或以上的设备上支持。使用单点登录,用户使用他们域管理的密码来登录隔离信箱而不使用梭子鱼上管理的密码了。建议启用此功能,使用户登陆梭子鱼用户隔离区更加简便,不用记忆梭子鱼的特有密码。

下表描述了相关设置:

登录 Realm 选择	如果启用此功能,在登录页面会显示一个 realm 选择下拉菜单,用户可以选择他们的 realm 来登录。
本地 Realm 名称	本地认证显示的 realm 名称(梭子鱼上建立的帐户和密码)
高级 single sign-on 设置	
Realm 名称	在登录页面,用户看到并可选择的 realm。在域设置页面一》编辑域时也可以看到。这是必须填写的。
认证类型	可用的认证类型有: Local (梭子鱼控制认证的帐户和密码) LDAP (在外部 LDAP 数据库上维护的密码) RADIUS(在 RADIUS 数据库上维护的密码) POP (在外部 POP 服务器上维护的密码)
认证主机	梭子鱼认证用户需连接的 LDAP,RADIUS,或 POP 服务器的 IP 地址。如果使用本地认证(梭子鱼),就不需要此设置。
认证端口	梭子鱼连接认证服务器使用的端口。
用户名模板	如果使用 LDAP 认证,这个区域包含梭子鱼防火墙绑定的用户名模板(如 cn=_username_,dc=mydomain,dc=com)。Username 使用完全的邮件地址和用户名部分替换。 如果使用 RADIUS 认证,这个部分应包含 RADIUS 共享的密码。
默认认证方式	决定了如果用户未选择一个 realm 或他们登录失败后,梭子鱼使用这个 realm 作为默认的 realm 来登录。

12 SSL 设置

启用 SSL:

启用 SSL 的目的通常是为了确保用户登录信息的安全。当你启用单点登录的功能时,也应该使用 SSL 功能,因为单点登录是以未加密形式把密码传送到梭子鱼。如果你不使用单点登录的话,那就不需要启用 SSL 功能。

SSL 协议不仅可以加密你的密码,也可以加密与 web 管理接口交换的数据。

只允许 HTTPS/SSL 访问	选择“是”，将只允许通过 SSL 方式访问管理界面。选择“否”，就使用标准的 HTTP 访问。注意：如果你启用 SSL，任何使用 HTTP 登录管理界面的用户会自动重定向到 HTTPS 等同的地址。
在邮件中使用 HTTPS 连接	决定了梭子鱼将包括在系统邮件中的链接以 https://显示。这会应用于从梭子鱼系统发送出的隔离邮件，系统报告和系统警告。这不应用于用户发送出去的邮件。
Web 界面 HTTPS/SSL 端口	梭子鱼防火墙使用的 ssl 端口。默认是 443。
证书类型	选择 SSL 认证的其中一项： 默认（梭子鱼网络）认证。这是梭子鱼网络免费提供的默认认证类型。 Private （由自己签名）：不需要从可信的 CA 购买认证。注意，同时需要下载 private 根证书并导入到你的浏览器中。 Trusted ：（已经 CA 认证）：可信的 CA 发行的认证。你的 web 浏览器通常可以识别，不需要另外的配置。
组织信息	
通用名称	访问管理界面的完整的域名。如：barracuda.yourdomain.com
国家缩写	两个字母的国家代码
州或省	你位于的州或省的全名
地区名	你公司位于的城市名称
单位或组织名	你公司的合法的名称
部门或科室	可选项，指定公司的部门
下载证书请求 (CSR)	下载一个 CSR 用来购买经授权认证中心签名的证书。证书的密钥长度为 1024 位。
下载私钥	下载一个私有证书的拷贝用于 CSR。授权认证中心(CA)要求提供一个你的私有证书。它只是在你下载了一个 CSR 后被用到。
下载 private 根证书	下载私有根证书并导入到你的浏览器设置中。如果你选择了私有证书认证类型，推荐下载。
上传私钥	
上传授权认证中心 (CA) 购买的证书	
上传标记证书	在使用 CSR 购买了认证证书后，点击浏览按钮找到它并点击上传。在上传你的证书后，要确认认证类型是 Trusted(上面描述的)。

13 区域关键字

在高级设置—》区域关键字页面，可以允许你增强梭子鱼检测中文和日文垃圾邮件的能力。

中国 (PRC) 大陆政策	中国大陆必须过滤的特殊关键字。
---------------	-----------------

中文垃圾邮件规则	若不能确定所收的邮件为中文,推荐"否"。 若收到的绝大多数为有效的中文邮件,推荐"是"。
日语垃圾邮件规则	若不能确定所收的邮件为日文,推荐"否"。 若收到的绝大多数为有效的中文邮件。推荐"Yes"。

14 通知邮件编辑

在高级设置—》通知邮件编辑页面，你可以修改通知邮件的默认语言。

当一份邮件被阻断时，梭子鱼会发送一个通知邮件给邮件接受者和发送者。**此通知包括了梭子鱼阻断邮件的简要的解释。你可以把梭子鱼防火墙管理员的联系信息添加到这里来，这样内部用户的邮件被阻断时，他可以联系管理员。**

梭子鱼在打开通知功能时，才会发送通知邮件。可以在基本设置—》垃圾邮件评分和基本设置—》病毒扫描页面来设置。

默认语言	选择发送通知邮件时使用的语言。你可以从这个下拉菜单中选择你使用的语言。修改后请保存。如果你定义通知邮件后，又改成之前定义的语言，那么你会失去所有自定义的信息。梭子鱼把通知邮件返回到默认设置。
文件被拦截 (给收件人)	当一份邮件包含被禁止的附件类型的文件时，梭子鱼会阻断此邮件，并发送此通知邮件给此邮件的接受者。
文件被拦截 (给发件人)	当有人发送包含被禁止的附件类型的邮件时，梭子鱼会阻断此邮件，并发送此通知邮件给此邮件的发送者。
垃圾邮件 (给发件人)	当梭子鱼因为确认是垃圾邮件而阻断邮件时，梭子鱼会发送此通知邮件给邮件的发送者。
病毒邮件 (给发件人)	当梭子鱼因为确认一份邮件包含病毒时，梭子鱼会发送此通知邮件给邮件的发送者。
%f	梭子鱼管理员的邮件地址（在邮件头的 from 区域）
%C	通知邮件的 cc 接受者地址
%d	RFC2822（当前时间）
%m	邮件 ID 的头区
%j	主题区
%s	The original envelope sender,rfc2821-quoted and enclosed in angle brackets
%S	接受发送者通知邮件的地址。通常是包含发送者邮件地址的列表，但是一些病毒会通过伪造来改变此地址。
%v	病毒检查程序的输出结果 the output of the virus checking program
%F	被禁止的文件名称

15 诊断工具

梭子鱼提供了几种诊断网络连接性的工具，但是可能影响梭子鱼的性能。

连接到梭子鱼中心	点这个按钮来建立一个连接到梭子鱼中心。这个连接将允许梭子鱼的技术支持工程师诊断并修理您的系统。
网络连接	
Ping	用这个按钮尝试 PING 一个主机或 IP 地址。请直接输入主机名或 IP。
telnet	用这个按钮尝试 Telnet 一个主机或 IP 地址。
Dig/NS-lookup	用这个按钮尝试 DIG (类似于 nslookup) 一个主机或 IP 地址。
TCP Dump	在梭子鱼上尝试执行 tcpdump 命令。
Traceroute	用这个按钮在梭子鱼上运行 traceroute 命令。

16 报表管理

生成系统报表：

梭子鱼有几种不同的报表可以帮助你跟踪系统检测到的垃圾邮件病毒邮件的发送者。你可以手动生成报表，也可以设置让系统每天自动发送报表。

显示或邮寄报表：

1. 在高级设置—》报表管理页面，在报表类型的下拉菜单中选择一个报表类型
2. 选择发送此报表的日期和时间
3. 完成以下工作：

邮 寄 报 表	输入每个接受者的邮件地址，点击邮寄报表，邮件地址之间用逗号隔开。每次只能发送一个报表。
显 示 报 表	选择显示报表，会占用很多系统资源。

自动发送每天的系统报告：

你可以在每个报告类型的地址栏输入接受系统自动产生的报表的用户邮件地址。

你可以在多个邮件地址之间用逗号隔开。如果你不想发送每天的报表，请不要在此报表旁的方框中输入邮件地址即可。

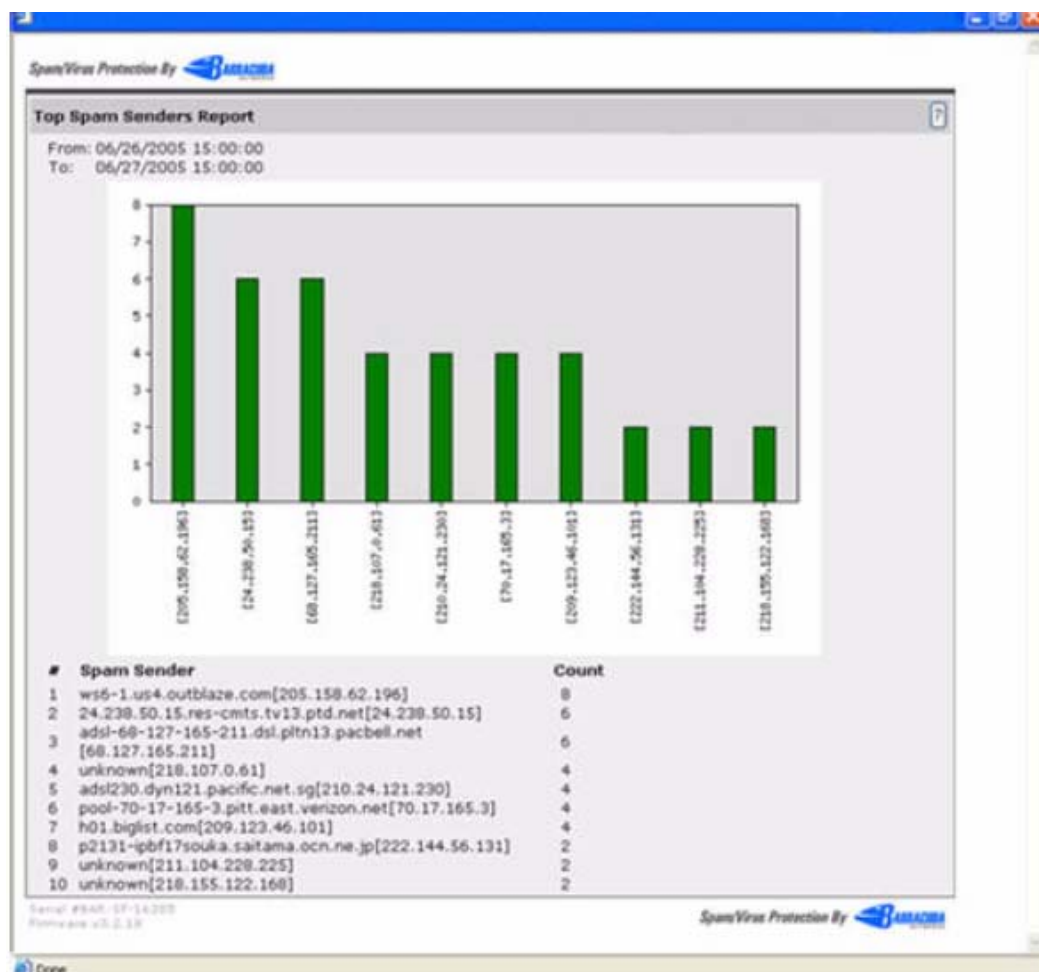
指定报表的属性：

你可以修改报表的属性来提高系统报表的有用性。

排行行数	报表中显示的前几名(如前 10 名邮件病毒)
------	------------------------

图表类型 每个系统报表的显示类型。支持的类型有圆形的，柱状的，水平的。

下表是一个垃圾邮件发送者的排序图表：



17 SMTP/TLS

当发送和接受的邮件服务器都是梭子鱼垃圾邮件防火墙或其中一台是支持 `starttls` 的邮件服务器时，启用此功能会将通过互联网的邮件加密以达到安全的目的。这个 SMTP 连接是以 STARTTLS 形式的 SMTP 命令来协商一个加密通道的。STARTTLS 是邮件通讯加密的一个标准的 SMTP 特性。

如果你选择“是”，进入和发出的连接都需建立 TLS 通道，且需要接受服务器支持此功能。

18 任务管理

你可以使用任务管理器来监控系统任务。梭子鱼跟踪的一些任务有：

- 集群环境设置
- 配置和贝叶斯数据的恢复
- 删除无效帐户

如果一个任务持续了很长时间还未完成，你可以点击任务旁的“终止”按钮，并且在系统负荷小的时候再来执行。任务错误部分将会列出一个错误，需要手动将其从列表中删除。

19 恢复控制台

替换一个出现故障的系统：

在替换梭子鱼设备之前，你可以使用梭子鱼提供的诊断工具（高级设置->诊断工具）来尝试解决你遇到的问题。

如果梭子鱼出现故障无法解决，并且客户购买了立即替换服务，那么请联系梭子鱼技术支持，你将在 24 小时内收到新的设备。

在接受到新的设备后，请把以前的设备返回到梭子鱼网络公司，地址如下。梭子鱼网络技术支持可以提供更加详细的信息：

Barracuda Networks

385 Ravendale Drive

Mountain View,CA 94043

注意：你可以在出现故障的设备上备份系统配置，贝叶斯数据库和用户配置。这样你将会快速的把数据导入到新的设备上。

重新启动系统来恢复：

如果你的梭子鱼出现了严重的故障而不能正常工作时，你可以使用系统的启动菜单的诊断和恢复工具来把系统恢复到出厂状态。

恢复之前需要做的事情：

- 使用系统内建的诊断工具来诊断问题
- 从最近的备份文件来恢复系统
- 联系梭子鱼网络技术支持进一步的解决问题
- 最后的方法是，重启梭子鱼系统进行内存测试或执行完全的系统恢复（下面描述的方法）

执行系统恢复或硬件测试：

1. 把键盘和显示器直接连接到梭子鱼设备上
2. 重启系统的两种方式：
 - 1) 在基本设置—》系统管理页面下方，点击重启按钮
 - 2) 在系统的前面板按电源按钮关闭系统，再按一次来启动系统。

梭子鱼显示的屏幕如下：

- ◇ Barracuda
- ◇ Recovery
- ◇ Hardware_test

3. 使用键盘来选择启动选项，并按回车键

你必须在 3 秒钟之内选择一个启动选项。如果你没有在 3 秒内选择一项，那么梭子鱼会以正常的模式启动（第一项）。

注意：可以通过键盘 ctrl-alt-del 组合键来停止硬件检测并重启系统。

Barracuda	以正常模式启动梭子鱼系统。如果在 3 秒钟内没有其他选择，梭子鱼会自动选择此项来启动系统。
Recovery	显示恢复的不同选项： 执行文件系统的修复—修复梭子鱼的 XFS 文件系统。只有你的梭子鱼的序列号在 24364 以下，才选择此项。否则的话，请选择“执行完全的系统恢复”。 执行完全的系统恢复—把梭子鱼恢复到出厂设置并清除隔离邮件，配置信息和贝叶斯数据库。 启用远程管理—打开反向通道，梭子鱼网络技术支持人员可以访问此系统。 另一种方法是在高级设置—>诊断工具页面点击连接到梭子鱼网络中心。 运行诊断内存测试—从操作系统中运行诊断内存测试。如果报告有错误，我们推荐运行下面的硬件测试。
Hardware_test	执行全部的内存测试，并会显示 2 小时内的内存相关错误。 要完成内存测试会持续很长时间。
	注意：恢复选项只在最新的梭子鱼型号上支持！

十. 梭子鱼外发模式

本章描述了梭子鱼外发模式的相关特征。其它章节中大部分的接收过滤模式的特征也适用于外发模式。但是以下的一些设置和页面只针对于外发模式的。

外发模式支持的一些页面如下：

基本设置—》邮件日志	在外发模式中提供了显示外发邮件的几种方法。
基本设置—》页脚	外发模式特有的
基本设置—》允许的发送者	外发模式特有的
策略	策略页面包含了很多接收过滤模式过滤设置的页面
高级设置—》邮件协议	此页面提供了一些外发模式特有的功能

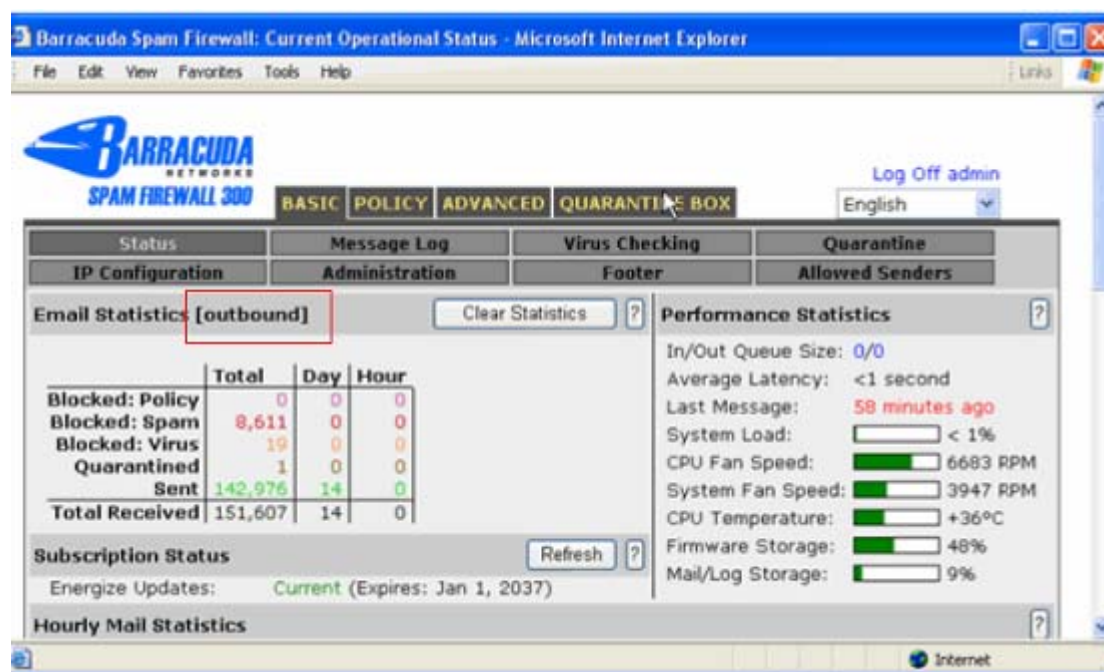
高级设置一》速率控制	在外发模式中一些不同的设置
高级设置一》信任转发	外发模式特有的
高级设置一》垃圾邮件评分	外发模式特有的
隔离信箱	外发模式特有的

关于外发模式：

外发模式保证向外发送的邮件是没有携带病毒和合法的邮件。它阻止了个别人员有意或无意利用公司网络来发送病毒邮件或垃圾邮件。**梭子鱼防火墙可以配置成接收过滤或外发模式，但不能同时配置两种模式。**

如果你把梭子鱼系统配置为外发模式，任何包含病毒的外发邮件都会被阻断且放到隔离信箱中。默认情况下，外发邮件不会进行意图分析或垃圾邮件评分，但是如果你需要，也可以启用此功能。

判断梭子鱼系统是外发或是接收过滤模式的简单方法是：在基本设置一》系统状态页面，在邮件统计的旁边显示出梭子鱼系统的模式。如下所示：



红色方框里表示此系统是外发模式。

在邮件日志中，查看外发邮件：

如果你的梭子鱼系统配置为外发模式，在基本设置一》邮件日志页面查看外发邮件的不同信息。

如动作列表包括：

发送—当外发邮件成功的发送到接受者的信箱时

放弃—当接受邮件服务器 down 机，接受者邮件地址不正确或是无效的时候

延迟—当超过速率控制的极限值时

动作列表也会在隔离或阻断由于违反策略的外发邮件时显示。其他的动作描述与接收过滤模式中描述的相同。

改变外发邮件的页脚:

默认情况下,梭子鱼会对所有外发邮件添加一个页脚。这个页脚告诉接受者此邮件已经被梭子鱼扫描了,是安全合法的邮件。

在基本设置-》页脚页面,可以改变默认设置。可改变的有:

添加页脚	决定了是否对外发邮件添加页脚
文本页脚	此页脚添加到文本或基于 ASCII 的邮件
HTML 页脚	此页脚添加到基于 HTML 的邮件
页脚排除	列出了添加页脚的发送者邮件地址。每行一个邮件地址。

指定允许的发送者:

在基本设置-》允许的发送者,可以控制哪些邮件被允许通过梭子鱼转发。你可以通过三种方法来控制:

1. 允许的发送域
2. 允许的 IP 地址
3. SMTP 认证

通过域和 IP 地址来指定允许的发送者:

下表描述了如何通过域和 IP 地址来控制发送者:

发送者的域	输入允许通过你的梭子鱼来发送邮件的每个域。输入后,点击添加按钮。如果你不填写的话,只有这里的地址被用来验证发送人邮件地址。
允许的发送者 IP 地址	输入允许通过梭子鱼发送邮件的每个 IP 地址或网络范围。如果你未填写的话: <ul style="list-style-type: none"> ✧ 所有 IP 地址都被允许通过梭子鱼发送邮件 ✧ 只使用允许的域来验证发送者

使用 SMTP 认证来指定允许的发送者:

如果你不使用 IP 地址或域来指定可以通过梭子鱼发送邮件,你也可以启用 SMTP 认证功能在梭子鱼发送邮件之前来认证用户。

如启用 SMTP 认证来控制允许的发送者,请填写以下内容:

基本设置-》允许的发送者页面

启用 SASL/SMTP 认证	支持的认证有: <ol style="list-style-type: none"> 1. None-关闭 SASL/SMTP 认证 2. LDAP-通过 LDAP 来进行认证 3. SMTP 认证代理-使用另一个 SMTP 邮件服务器来认证。因为梭子鱼是以明文形式传送密码的,所以建议配置加密方式: 高级设置-》SMTP/TLS。
编辑 LDAP 设置	如果你使用 LDAP 认证,那么请输入你的 LDAP 服务器的相关信息。
SMTP 认证服务	如果你使用 SMTP 认证方式,请输入认证服务器的地址。

器	用户提供的用户名和密码将通过 SMTP 认证命令转发给这台 SMTP 服务器。它可以是任何支持 SMTP 认证命令的服务器,比如微软的 Exchange 或者 Sendmail。
---	---

外发模式的其它邮件协议设置:

外发模式的梭子鱼包含其他的设置,你可以在高级设置—》邮件协议页面设置。如下:

最大邮件大小	决定了梭子鱼可以接受的最大邮件大小(单位:字节)。超过此限制的邮件会自动被阻断并发送一个不可达的通知给发件人。
每个 SMTP 会话的邮件数量	限制一个 SMTP 会话允许的邮件数。如果一个会话的邮件数超过了此限制,那么其它的邮件会被阻断。在邮件日志显示为延迟,原因是每连接邮件数限制。发送者需要重新建立一个连接来发送邮件。

启用意图分析和垃圾邮件评分:

默认情况下,意图分析和垃圾邮件评分在外发模式下是关闭的。如想启用此功能,请到高级设置—》评分设置和贝叶斯/意图分析页面启用这两项功能。

标记分值	外发模式下,垃圾邮件评分默认是关闭的。如果你启用垃圾邮件评分,确定也要配置隔离和阻断分值。
隔离分值	邮件的评分超过此分数,低于阻断分数,那么邮件都会被转发到隔离信箱中。
阻断分值	邮件的评分超过此分数,那么都会被梭子鱼阻断并发送一个弹回通知给发送者。
意图分析	当意图分析启用时,梭子鱼会对外发邮件中包含的 URLs 到本地数据库中检查,验证它是否总是发送垃圾邮件。如果梭子鱼找到匹配的 URLs,那么此邮件会被自动阻断。外发模式默认是关闭意图分析的。 <i>注意: 包含 URLs 地址的本地数据库是会动态更新的。</i>
免除 URL 地址	这些 URLs 都不会被分类为可疑的,即使在意图分析时发现此地址。建议输入你外发邮件中通常包含的 URLs。 <i>注意: 输入 URLs 时,不需包括“http://”。</i>
弹回通知	默认情况下,当邮件被阻断或未发送出去时,梭子鱼将发送一个弹回通知给发送者。如果你选择“否”,那么将关闭此功能。

管理隔离信箱:

当梭子鱼在外发邮件中检测到病毒时,此邮件会被自动放到隔离信箱中。这样系统管理员可以采取合适的措施(如对发送者的计算机进行病毒扫描)。如果启用了垃圾邮件扫描功能,那么垃圾邮件也会自动发送到隔离信箱中。

隔离邮件时发送弹回通知:

在梭子鱼隔离一份邮件时,它将发送一个弹回通知给发送者,告诉他们这些邮件未发送出去。如果当外发邮件被隔离了,不想让梭子鱼发送弹回通知。你可以在基本设置—》隔离页面,

设置此项为“否”

显示和分类隔离邮件：

在隔离信箱页面，列出了梭子鱼已经隔离的邮件。如查看一份邮件的内容，请点击此邮件。在隔离信箱中查看邮件后，你也可以从隔离信箱中删除此邮件或发送到实际的接受者。下表详细列出了你可采取的动作。

发送	发送此邮件到目的接受者。 <i>注意：如果在邮件中检测到病毒了，你还要发送，那么此病毒不会被删除。</i>
白名单	将邮件的发送者地址加入到白名单中并发送此邮件。此发送者以后发送的所有邮件都不会被隔离。
删除	从隔离信箱中将此邮件删除。
拒绝	发送一个弹回通知给发送者并将此邮件从隔离信箱中删除。
转发	转发此邮件到一个特殊的地址。当你在另外一个系统上进一步检查此邮件时，可以转发此邮件。

使用过滤条件来搜索邮件：

如果你的隔离信箱中有很多邮件，那么你需要使用过滤条件来搜索指定的邮件。这些过滤条件包括：

From 包含—在所有隔离信的 from 区域搜索你定义的内容

主题包含—在所有隔离信的主题行搜索你定义的内容

邮件包含—在所有隔离信的信件中搜索你定义的内容

如果邮件日志非常大的话，有时搜索可能不成功或占用很长时间。

配置邮件的速率控制：

速率控制可以允许你配置在半小时内从同一个 IP 地址发起的连接数。速率控制可以阻止垃圾邮件发送者在短时间内发送大量的邮件到你的服务器。下表描述了相关设置：

速率控制	指定了速率极限： 在半小时内从同一个地址发起的最大连接数。这个设置在有 5 个不同的 IP 地址连接到梭子鱼时才会生效。 同一个邮件地址的最大 SMTP 会话数。这个设置在有 5 个唯一的邮件地址已经被发送后才会生效。 当连接数或 SMTP 会话数超过了极限值时，梭子鱼会阻断从那个 IP 地址发送来的邮件以及 SMTP 会话。
速率控制排除 IP 区间	输入你想排除速率控制的 IP 地址范围。如果你输入一个 IP 地址，请使用此掩码：255.255.255.255。
速率排除的邮件地址	在这里输入的邮件地址都不会被速率控制。每行一个邮件地址。

添加一个转发服务器：

在高级设置—信任转发页面，你可以为一个域添加转发服务器或 Smart 主机。如果你想把一个域的邮件重定向到另一个转发服务器或另一个邮件服务器上，你需要添加一个转发服务

器。

添加转发服务器：

1. 在转发服务器配置区域，输入转发服务器域名并点击添加域。
2. 输入转发服务器的 IP 地址和目标端口
3. 确定是否使用 MX 记录
4. 点击保存按钮
5. 输入一个有效的邮件地址，点击测试按钮
6. 梭子鱼会发送一份邮件到转发服务器上
7. 在转发服务器上检查是否收到测试邮件。如果未收到，请检查一下你输入的信息是否正确。

如果你把所有的邮件都定向到一个转发服务器上，按照以下设置：

1. 输入*号作为域名，点击添加域
2. 在域名列表中点击每行旁边的删除按钮来删除所有其他的记录

这个*号，将会使所有转发到梭子鱼的外发邮件都发送到另一个转发服务器上，这个转发服务器是在高级设置—》转发设置页面来配置。

设置主题和信体过滤：

你可以使用按钮来过滤包含信用卡，信息，秘密或 HIPAA 信息的机密或敏感材料的外发邮件。**These buttons contain pre-set patterns.**当你选择后，他们被以代码形式作为关键字嵌入到规则表达式中。包含这些关键字的外发邮件将被阻断。这些信息包括：

信用卡：通过梭子鱼外发模式的垃圾邮件防火墙发送出去包含 `master card,visa,American express,diners club` 或 `discover card numbers` 的邮件将会阻断或隔离。

社会安全：具有有效社会安全号码的外发邮件会被阻断或隔离。

秘密：如果邮件中包含两个或更多以下信息（地址，生日，身份证号码，信用卡号码，汽车牌照，电话号码或过期日期），此邮件会被阻断或隔离。

HIPAA：如果邮件属于秘密或包含两个或以上的私有医疗信息的邮件也会被阻断或隔离。

这些形式都可以最小化滥用机密信息，但是也不能完全保证准确性和完全阻止滥用机密信息。让你公司员工认识到什么是滥用机密信息是非常重要的。

附一. 梭子鱼常见问题 Q&A

什么是垃圾邮件评分，贝叶斯学习，邮件指纹识别？

- 1) 所谓垃圾邮件得分是指与一个大约有四千条规则的系统与邮件进行特征比对后的得分。得分的高低决定对邮件如何处理。但对后面的分析没有直接的作用。规则库需要动态更新。
- 2) 贝叶斯分析也产生垃圾邮件得分。在邮件日志中，您标记邮件为垃圾或非垃圾时贝叶斯分析也被用到。
- 3) 博威特中心清算所利用指纹识别技术可以准确并且充分的识别出垃圾邮件。当一份邮件被鉴定为垃圾邮件后，将被送往博威特中心清算所并被提取邮件指纹。

全局隔离设置与分用户隔离设置的根本不同是什么？

全局隔离设置允许系统管理员指定一个邮箱用来接收所有的隔离邮件，管理员可以访问该邮箱并对隔离邮件进行相应的处理。分用户隔离设置是在梭子鱼上为每个用户建立一处隔离店铺，每个用户都将收到一份个人化的垃圾邮件隔离概要的邮件，通过该份概要用户可以选择接受或删除隔离邮件，或者设立黑白名单。

全局和分用户垃圾邮件隔离概要什么时候发出？

每天下午 3:00 左右。

能够同时选择全局和分用户两种隔离类型吗？

不行，任一时刻，这两种类型只能选其一。

除了通过 web 界面访问垃圾邮件防火墙操作系统外，是否还有别的方式如 telnet 或 ssh？

Web 界面提供给简单友好的配置界面。除此之外，梭子鱼不提供其他的会话方式。

可否配置梭子鱼能将分类为垃圾的邮件复本投递到一个邮箱中？（不为隔离，仅为转移）

梭子鱼允许所有的隔离邮件投递到某个邮箱中。

不同的邮件用户或邮件域用户可否设置不同的垃圾邮件检测、等级及阻断策略？

梭子鱼 300 及以上型号支持分用户设置，用户可通过隔离通知邮件管理隔离邮件。管理员制定初

始策略，用户可修改策略，但管理员拥有最终修订权。

能否设置垃圾邮件防火墙能够针对发件人 DNS 域进行反垃圾检查？

梭子鱼利用 DNS MX records 查找进行处理。

如何更新垃圾邮件规则和病毒特征码？

梭子鱼动态更新功能可设置自动更新垃圾邮件规则库和病毒特征码。用户可设置每小时或每日更新，通常设置为每日更新。

梭子鱼垃圾邮件防火墙对域的支持数量有限制吗？

一般不超过 500-2000 个，各个型号之间有差异。

梭子鱼垃圾邮件防火墙能否设置多域过滤邮件。

可以，在高级页—高级域设置中可设置多目标服务器及多域。

能否将博威特垃圾邮件防火墙与邮件服务器设置在不同的子网中。

可以。只要有正确的路由，无论是否在同一个子网，邮件经梭子鱼处理后最终能送达邮件服务器。进入梭子鱼管理界面，选择基础页设置目的邮件服务器的 ip 地址或服务器名即可。

若用户有两个用户名能进入同一个邮箱，是否两个用户名都要禁用。

是的。用户名必须唯一，这样他才能进行个性化设置。

梭子鱼 400 和 600 为什么提示：Redundant Drive (RAID) Status: 警告-在单磁盘中运行？

这通常表示在非正常关机或重新启动后及第一次使用初始化时系统正在重建 RAID 阵列。一般 24-36 小时后提示消失。

为什么 WEB 管理界面上梭子鱼防火墙的更新及动态更新都没升级？

请检查梭子鱼的默认网关其 80 端口是否对 internet 开放。检查所有的网关 80 端口是否开放。

在邮件日志上看到动作为“允许”，原因为“邮件尺寸”是什么意思？

如邮件尺寸过大，超过内部设定的最大值（通常为 64k），该邮件将被允许。

如何阻断来自国外的域如：.de .uk .il ？

在发件人域阻断/接受设置中添加 de uk il 即可。

如何验证 LDAP 启动？

在 web 管理界面高级页/MS Exchange 加速器下用一个账号测试一下。

高级页防火墙更新中出现如下信息是什么意思？

Warning: Firmware update server unreachable for one of the following reasons:

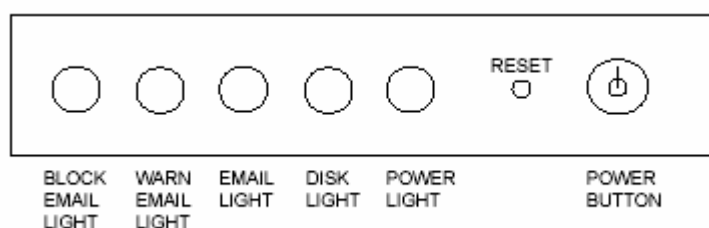
- *The primary and/or secondary DNS servers are misconfigured*
- *The Spam Firewall is unable to route to the internet because of its IP/Gateway configuration*
- *The Spam Firewall is unable to communicate with the update server (update01.barracudanetworks.com) on port 80 due to your firewall configuration*

警告：梭子鱼防火墙因为下列原因不能访问：

- 主从 DNS 服务器未设置。
- 因 IP 或网关配置不当垃圾邮件防火墙无法访问 internet。
- 因为您的防火墙的未开放梭子鱼垃圾邮件防火墙 80 端口故不能与更新服务器（update01.barracudanetworks.com）通讯。

解决办法：检查并设置好网关，检查 DNS，确定防火墙开放梭子鱼的 80 端口。

梭子鱼防火墙前方面板上的指示灯标示似乎与灯的指示含义不符？



答：可能是运输途中造成前方面板脱落用其他面板代替造成的。

梭子鱼垃圾邮件防火墙 (BSF) 安装完成后会不会造成邮件收发延时？

答：梭子鱼垃圾邮件防火墙具有强大的邮件处理能力，以 BSF 300 型号为例，日处理能力为 400 万封邮件，即处理每封邮件仅需约 0.02 秒，对于实时性要求不高的电子邮件来说，完全可以忽略不计。

梭子鱼垃圾邮件防火墙使用的是何种病毒引擎。

答：梭子鱼采用open source的防毒引擎第一次过滤拦截绝大部分病毒，梭子鱼原创防毒引擎在作第二次过滤。

什么是 DoS 和 DDoS 攻击？

答：DoS 是 Denial of Service 的简称，即拒绝服务，造成 DoS 的攻击行为被称为 DoS 攻击，其目的是使计算机或网络无法提供正常的服务。最常见的 DoS 攻击有计算机网络带宽攻击和连通性攻击。带宽攻击指以极大的通信量冲击网络，使得所有可用网络资源都被消耗殆尽，最后导致合法的用户请求就无法通过。连通性攻击指用大量的连接请求冲击计算机，使得所有可用的操作系统资源都被消耗殆尽，最终计算机无法再处理合法用户的请求。

分布式拒绝服务(DDoS:Distributed Denial of Service)攻击指借助于客户/服务器技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动 DoS 攻击，从而成倍地提高拒绝服务攻击的威力。通常，攻击者使用一个偷窃帐号将 DDoS 主控程序安装在一个计算机上，在一个设定的时间主控程序将与大量代理程序通讯，代理程序已经被安装在 Internet 上的许多计算机上。代理程序收到指令时就发动攻击。利用客户/服务器技术，主控程序能在几秒钟内激活成百上千次代理程序的运行。

我有问题怎么和梭子鱼的技术支持取得联系？

答：你首先可与您当地的代理商联系，如果他们不能解决的问题，你也可以直接联系博威特（上海）有限公司取得联系，咨询我们的中国区技术支持中心。技术支持电话 021-54520368 转售后技术支持。或发邮件描述您的问题到 support@barracudanetworks.com.cn。你也可以直接联系我们的 24 小时全天候国际技术支持中心请求他们的帮助，他们的电话为 (408) 342-5444，邮箱为：support@barracudanetworks.com。你还可以登陆我们的技术支持论坛 <http://www.barracudanetworks.com.cn/bbs> 进行提问，我们的技术人员将会详尽为您解答。

我无法打开机器的“邮件日志”？

答：出现这种问题一般是由于您在群集（Clustering）中的 IP 地址没有更新所致，请将您现使用的 IP 地址设置使用，并为活动的（Active）一般就能解决此问题，如还不能打开请使用界面提供的重启按钮正常启动机器便能打开。

我的界面是英文的，并且无法升级到中文？

答：请看您的系统内核(Firmware)版本，一般 3.0.X 的版本以上，都有多种语言界面并且能自动显示成中文。如果您不是这些版本，而且内核升级界面中显示的最高版本也不能升级到 3.0.X 版本或之上，请立即与我们的技术人员取得联系，我们将为您解决此类问题。

我在第一个页面看到的系统性能统计数据页中，发现有部分红色部分绿色的条框，请问是什么意思？

答：绿色条框是正常状态的显示，红色条框则表明目前的机器在本方面的状态处于非常规状态。比如，邮件日志达到百分之九十以上时会显示红色警告当前日志将满；机器风扇转速过高或过低，CPU 温度过高或过低都会显示红色条框提示警报。此时应作相应的处理。

我的邮箱帐号是否保存在梭子鱼机器内，如果梭子鱼产品当机，是否会影响我的邮件帐户的正常使用？

答：你的邮箱时保存在你的的邮件系统中的，梭子鱼产品的一些功能，如：拒绝字典攻击等，只是保存了一个您帐户的动态列表。梭子鱼产品在使用中如果意外死机，不会损坏您的邮件系统和邮箱帐户等。如您需要撤下梭子鱼产品，只需重新更改您的 MX 指向。

梭子鱼要求 SMTP 握手是什么意思？

邮件服务器连接的时候通常第一个 smtp 命令是 hello，也就是要求握手，hello 相当于向对方表明自己的身份。

如果设置，效果怎么样？

若设置必须握手，则如果第一个命令不是 hello 将拒绝接受邮件

在梭子鱼管理界面用户管理页中，很多用户都是我们服务器中没有的，怎么才能批量删除啊，好象删除作废帐号按钮没什么用嘛！

284871548.28325@njau.edu.cn 284938999.25904@njau.edu.cn 285573731.14483@njau.edu.cn
285577261.14640@njau.edu.cn 287275160.31658@njau.edu.cn 287530918.05675@njau.edu.cn
289640934.01039@njau.edu.cn 289804573.32136@njau.edu.cn 293509836.17774@njau.edu.cn
这些帐号都不存在啊！怎么批量删除呢？

用用户管理页中最下面的 remove 无效用户 按钮

不过，要将 exchange 加速器关掉才能生效。这时，梭子鱼收到邮件时会用 smtp 命令与邮件服务器查询收件人是否存在，不存在的话就认为是非法邮件而阻断。使用 remove 按钮删除无效用户的原理也是如此。

而采用 exchange 加速器时，梭子鱼采用的是 ldap 查询收件人方式，所以就不能用 remove 按钮删除无效按钮了

4 还有，系统每天都发垃圾邮件统计给我，但好象只发了一次，已经很多天没有收到了！

那些用户很多都是假帐号！

3.1.01 中报告设在高级--> 的 report 中，你到哪里加一下

增加了好几种报告类型，如垃圾邮件发送者排名报表、病毒邮件排行榜等

何谓梭子鱼的意图分析/目的分析？

目的分析通过查看邮件中的 URLs 分析邮件的意图。博威特中心维护着一份人工分拣出的垃圾邮件发送者的网站 URLs 地址，并且不断地进行更新。

这些 URLs 地址来源于垃圾邮件。博威特设置了大量的“蜜罐”来收集这些地址，同时各地的梭子鱼垃圾邮件防火墙也可以收集并发送垃圾邮件给我们，用户可以在基本->贝叶斯/邮件指纹->提交邮件中选择“是”就可以将垃圾邮件的副本发给我们。

我们分析的邮件包括多种不同的语言，博威特中心能够流利的使用以下几种语言：

英语，荷兰语，日语，德语，法语，西班牙语，葡萄牙语，中文简体，中文繁体，越南语，菲律宾语。

但是需要注意的是，为了破坏意图分析过滤，有些垃圾邮件中故意添加一些绝对不可能发送垃圾邮件的网站 URLs，如 w3.org；或者垃圾邮件链接如 DOC 文档以绕过意图分析。

分用户隔离设置是怎么回事？

梭子鱼垃圾邮件防火墙 300 及以上型号支持分用户隔离设置，这篇文档帮助读者理解该项设置。

分用户隔离与全局隔离

过去梭子鱼仅支持全局隔离设置，即允许用户在邮件服务器上设置一个账号接受所有的隔离邮件，自 1.9.0 版本以后，梭子鱼开始支持分用户隔离邮件设置，即用户可以登陆梭子鱼防火墙直接管理他们的隔离邮件，同时也可以的它的账号进行相关设置。分用户隔离设置不是默认设置，用户需在 web 界面启动该项功能。

分用户隔离的功能

梭子鱼设置为分用户隔离时，若收到隔离邮件，梭子鱼将把隔离邮件存在梭子鱼上的某个帐户中，等待用户接收。如果某用户第一次收到隔离邮件，梭子鱼将自动设置一个隔离账号并向该用户发一封欢迎邮件。

在这封欢迎邮件中，含有一个链接，用户打开后可以登陆梭子鱼，这样就可以查看隔离邮件的内容了，用户还可以将隔离邮件进行分类为垃圾或非垃圾邮件，允许或阻断某个发件人，更改接收隔离通知邮件的时间，以及修改密码。

设置隔离

系统缺省设置关闭隔离，登陆 web 管理界面，进入基础->垃圾邮件评分，设置隔离得分小于阻断得分；如果需要，用户可以关闭标记，这样梭子鱼的邮件只进行隔离或阻断；如果用户启用标记，请注意隔离得分要大于标记得分小于阻断得分。这样全局隔离功能就自动启用了。

设置隔离类型

进入 web 界面基础->隔离中，您可以设置不同的隔离类型，说明如下：

隔离类型：您可以设置隔离类型为全局或分用户。

全局隔离配置：您可以设置隔离邮件发送到哪一个邮箱，还可以设置隔离标记文字，他将被添加在隔离邮件主题中。

分用户隔离配置：你可以设置一个邮件地址，发送隔离通知，以使用户访问隔离邮件，您也可以设置隔离通知发送的周期。

分用户隔离账号管理：您可以设置某些用户启用或关闭分用户隔离功能，而这些用户的名单您可以在下方的文本框中输入。

梭子鱼中关于使用表达式的说明

在梭子鱼中，用户可以用表达式表示某个文本过滤关键字，用户可以在阻断/接受—点“？”—点“表达式规则”。

表达式的使用不是必需的，在使用特殊符号，如|, *, '.'请注意使用规则。

以下是梭子鱼表达式使用的一些规定

大小不敏感

表达式说明

表达式是由字符、字符组及算术符号联结起来的。

算术符号说明：

- * - 0 及以上
- + - 1 及以上
- ? - 0 或者 1
- | - or
- () - 分组

字符组说明：

梭子鱼中以 '[' 和 ']' 括起来的表示某字符组，用 “-” 表示字符区间，用 ‘^’ 表示否定。

例如：

- . - 除去新行的任何字符
- [ac] - 字母 'a' 或者字母 'c'
- [^ac] - 除字母'a' 及字母 'c'外的任何字母
- [a-z] - 字母'a' 到字母 'z'
- [a-zA-Z.] - 字母 'a' 到'z' 或者 'A' 到 'Z'或者.
- [a-z\ -] - 字母'a'到 'z' 或者 -
- \d - 数字, 代表 [0-9]

- **\D** - 非数字,代表 $[\text{^0-9}]$
- **\a** - 数字, 代表 $[\text{0-9}]$
- **\w** - 部分单词: 代表 $[\text{A-Za-z0-9_}]$
- **\W** - 非单词字符: 代表 $[\text{^\w}]$
- **\s** - 空间符号:代表 $[\text{\n\r\t}]$
- **\S** - 非空间符号: 代表 $[\text{^\s}]$

杂项

- **^** - 行开始
- **\$** - 行结束
- **\b** - 文字边界
- **\t** - 制表符

特殊符号

下列符号在表达式重中具有特殊含义，在使用时前面要用\。

.
[
]
\
*
?
\$
(
)
|
^
@

例子

- **viagra** - 匹配 viagra, VIAGRA 及 v1aGRa
- **\d+** - 匹配 1 或者更多数字 s: 0, 42, 007
- **(bad|good)** - 匹配单词'bad'或者匹配单词'good'.
- **^free** - 在行的开始处匹配单词'free'
- **v[i1]agra** - 匹配 viagra 或者 v1agra
- **v(ia|1a)gra** - 匹配 viagra 或者 v1agra
- **v\|agra** -匹配 v|agra
- **v(i|1|\|)?agra** - 匹配 vagra,viagra, v1agra 或者 v|agra
- ***FREE*** - 匹配 *FREE*
- ***FREE* V.*GRA** - 匹配 *FREE* VIAGRA, *FREE* VEHICLEGRA, 等.

贝叶斯过滤是如何评分的？

梭子鱼专门针对邮件病毒进行过滤，有些病毒不通过邮件传播却可能攻击系统，例如 MS blaster，梭子鱼及时提供系统补丁进行防御，截至目前梭子鱼可处理 23166 种邮件病毒。

从美国用户收集来的贝叶斯的评分情况如下：

Bayes scores

```
0.00 BAYES_50 BODY: Bayesian spam probability is 50 to 56%
[score: 0.5524]

2.10 BAYES_90 BODY: Bayesian spam probability is 90 to 99%
[score: 0.9832]

5.40 BAYES_99 BODY: Bayesian spam probability is 99 to 100%
[score: 0.9927]

-0.90 BAYES_30 BODY: Bayesian spam probability is 30 to 40%
[score: 0.3379]
```

```
4.90 BAYES_00 BODY: Bayesian spam probability is 0 to 1%
-1.52 BAYES_01 BODY: Bayesian spam probability is 1 to 10%
-0.91 BAYES_10 BODY: Bayesian spam probability is 10 to 20%
-1.43 BAYES_20 BODY: Bayesian spam probability is 20 to 30%
-0.00 BAYES_44 BODY: Bayesian spam probability is 44 to 50%
0.00 BAYES_50 BODY: Bayesian spam probability is 50 to 56%
0.00 BAYES_56 BODY: Bayesian spam probability is 56 to 60%
1.59 BAYES_60 BODY: Bayesian spam probability is 60 to 70%
2.25 BAYES_70 BODY: Bayesian spam probability is 70 to 80%
1.66 BAYES_80 BODY: Bayesian spam probability is 80 to 90%
2.10 BAYES_90 BODY: Bayesian spam probability is 90 to 99%
5.40 BAYES_99 BODY: Bayesian spam probability is 99 to 100%
```

附二. 常见错误邮件信息列表

Message Logs Statements

类型	错误编号	原因
RBL message	554	外部黑名单 External Blacklist.
Rate Control Messages	554	连接数过多 Too many connections. 消息过多 Too many messages. 速率控制 Rate control.
Timeout message	421	中断 Abort. 发件人超时 Sender Timeout
No such domain message	550	不存在的域 No such domain. 非法域 Invalid domain.
No such user message	550	不存在收件人 No such user. 非法收件人 Invalid recipient.
Blocked subject message	550	主题非法 Illegal subject containing "(.*)". Subject.
Blocked body message	550	信体非法 Illegal message body containing "(.*)"
Blocked ip message	550	拒绝发件人主机 Client host rejected. Client
Blocked sender message	550	拒绝发件人地址 Sender address rejected. Sender.
Blocked recip message	550	收件人地址拒绝 Recipient address rejected. Recipient.
No valid recipients message	554	不存在的收件人 No valid recipients.
Fake domain message	450	拒绝发件人地址, 域没有找到, 虚假发件人域。Sender address rejected. Domain not found. Fake sender domain.
Busy message	451	系统繁忙中 Server undergoing. System busy.
Recipient fqdn required	504	收件人需要完整合法的域名, 收件人域名必须。Recipient needs fully qualified domain. Recipient domain name required.
Sender fqdn (正式域名) required	504	发件人需要完整合法的域名, 发件人域名必须 Sender need fully qualified domain. Sender domain name required.
Unsupported error	555	无法支持, 违反邮件协议()Unsupported. Mail Protocol Violation (unsupported option).
Mail from error	501	违反邮件协议 Mail Protocol Violation (MAIL FROM command expected).

Mail from error	501	Mail Protocol Violation (RCPT TO command expected).
Helo required	503	违反邮件协议 Mail Protocol Violation (HELO/EHLO required).
MAIL FROM required	503	Mail Protocol Violation (MAIL command required)
Nested MAIL required	503	Nested MAIL. Mail Protocol Violation (Multiple MAIL FROM commands)
Bad syntax	500	Bad syntax. Mail Protocol Violation (bad syntax).
Unknown command	502	Mail Protocol Violation (disconnect, not delivered).
Abort message		发件人放弃 Sender abort.
Abort message		发件人退出 Sender quit.

附三. 常见有限保修、快速替换和动态更新服务问题解答

动态更新服务

什么是动态更新服务？

为了最大限度地保护您免受最新安全漏洞的袭击，博威特网络技术（上海）有限公司持续不断地检控网络垃圾邮件和病毒攻击的最新趋势。我们汇编了动态更新来更新我们的产品使它免受各种层出不穷的新型攻击。动态更新直接导入博威特的产品之中并提供最新垃圾邮件和病毒定义。您可以根据您的系统配置来决定是每小时还是每天运行更新。动态更新需向博威特网络技术（上海）有限公司购买，分别有一年、三年和五年期限可供选择。当您的动态更新到期，请根据当时的报价续费。

为什么动态更新服务需要购买？

因为病毒和垃圾邮件的攻击是不断变化的所以动态更新服务是博威特产品不可分割的部分。

有限保修

有限保修包括那些内容？

该有限保修包括原材料和工艺上缺陷。

有限保修不包括那些内容？

该有限保修不包括：

外部客观原因如意外事故、滥用、误操作和电源问题

未经博威特网络技术有限公司授权私自维修

不按照使用手册使用产品

错误理解博威特网络产品使用手册或错误执行预防性维护

由于使用非博威特网络技术(上海)有限公司提供的附件、零件或其他组成部分而引起的问题
产品序列号被遗失或更改

未支付货款的博威特网络产品

产品为“样品”、“测试版”、“样机”或“试用版”

租赁或免费提供的产品

有限保修的期限是多久？

有限保修自发票日期起1个月包换，一年内保修。如果您是通过代理商购买的博威特网络产

品，则保修期自该销售公单位开具的发票日期起为1个月包换，一年保修。

当我需要保修服务时该找谁？

如果您直接从博威特网络技术（上海）有限公司购买产品：

请在保修期到期前联系博威特网络技术（上海）有限公司要求提供保修服务并提供有效产品序列号。电话**(8621) 54520358** 或**(8621) 54520368**，工作时间为周一至周五的上午9点到下午5点（太平洋标准时间）。

如果您从代理商处购买产品：

请在保修期到期前联系您的代理商。您的代理商会协调原产品退回、修理或更换事宜，并负责将产品返还给您。如果您还没联系代理商，也可以选择直接与博威特网络技术（上海）有限公司联系保修服务事宜。

保修期内的保修程序是怎样的？

在一年保修期内，博威特网络技术（上海）有限公司负责维修那些被确认为是原材料和工艺缺陷而退回的博威特网络产品。如产品不可修复，则由新的或翻新的相当产品替代。如被确认为非保修范围内，则通知您选择可提供的服务。

在保修期内如何退回需要保修的产品？

当您联系博威特网络技术（上海）有限公司或其授权代理商时，将给您一个退回产品许可号 [RMA Number] 来退回产品。您必须退回所有原装产品，并支付运输费和运输保险费。请注意必须将RMA number标注于外盒上，然后我们将返还给您维修或替换的产品。

谁来承担运费？

您负责支付退回产品的运费；如果您居住在中国，博威特网络技术公司或其分销商负责返还维修或替换产品的运费。

在保修期内怎样收取替换产品？

如果您购买了快速替换服务，博威特网络技术（上海）有限公司将在收到您退回的原包装产品的七个工作日内为您发出替换产品。

如果您未购买快速替换服务，则由博威特网络技术（上海）有限公司负责送回原产地维修后退还。

保修期是否因产品被修理或替换而延长？

保修期不因产品被修理或替换而延长。

保修期结束后怎么办？

一年有限保修期到期后，博威特网络技术（上海）有限公司负责维修您的产品。您必须退回所有原包装产品，并支付运费和运输保险费。请按以下说明支付维修费，维修时间取决于故障严重程度，一般来说大约需要两周。以下列出的是保修期外的维修价目表：

Barracuda Spam Firewall 200: ¥3300

Barracuda Spam Firewall 300: ¥5000

Barracuda Spam Firewall 400: ¥6700

Barracuda Spam Firewall 600: ¥12500

博威特网络技术（上海）有限公司将怎样修理我的产品？

在将产品退还给您前，博威特网络技术（上海）有限公司将完全彻底地检测校验您的产品确保其已正常运作。博威特网络技术（上海）有限公司使用原厂生产的新的或翻新零件进行保修。翻新的零件和系统是指那些被退回到博威特网络技术公司的零件和系统，有些尚未被使用过。所有零件和系统都经过品质检查和测试。替换零件和系统用于保修期内的产品，所有替换零件都来自于返修产品，博威特网络技术有限公司将给您与原产品相当的替换品。

快速替换服务

什么是快速替换服务？

快速替换服务是一个工作日内发出替换产品的服务计划，当您的产品发生任何问题时，便可启动该服务计划。快速替换服务自到期后续费，分别有一年、三年和五年期限可供选择购买。

快速替换服务的期限是多久？

快速替换服务自博威特网络技术（上海）有限公司发票日期起计算，根据您购买的服务计划分别为一年、三年和五年。如果您是通过代理商购买博威特网络产品，则快速替换自该销售单位开具的发票日期开始计算。

如果我在购买梭子鱼产品时没有购买快速替换服务，可以后续购买吗？

在您购买博威特网络产品30天内，您可以决定是否购买快速替换服务。如果您在这30天内决定购买快速替换服务，那么该服务期回溯到产品发出日起，根据您购买的服务计划计算服务期。

哪些情况不适用快速替换服务？

以下情况不适用快速替换服务：

外部客观原因如意外事故、滥用、误操作和电源问题

未经博威特网络技术有限公司授权私自维修

不按照使用手册使用产品

错误理解博威特网络产品使用手册或错误执行预防性维护

由于使用非博威特网络技术（上海）有限公司提供的附件、零件或其他组成部分而引起的问题
产品序列号被遗失或更改

未支付货款的博威特网络产品

产品标记为“样品”、“测试版”、“样机”或“试用版”

租赁或免费提供的产品

怎样使用快速替换服务？

如果您直接从博威特网络技术（上海）有限公司购买产品：

如果您的产品在快速替换服务期内发生故障，请联系博威特网络技术（上海）有限公司获取产品退回许可号，我们将在收到完整原包装产品后的七个工作日内通过合理的商业快递和邮寄方式把替换品发送给您。

如果您从代理商处购买产品：

如果您的产品在快速替换服务期内发生故障，请联系您的代理商取产品退回许可号。您的代理商将在收到完整原包装产品后的七个工作日内通过合理的商业快递和邮寄方式把替换品

发送给您。

如果您还没联系代理商，也可以选择直接与博威特网络技术（上海）有限公司联系产品替换和原产品退回事宜。

我可以转让有限保修、快速替换服务或动态更新服务吗？

有限保修、快速替换服务和动态更新服务属于原始用户，并不得在任何情况下进行转让。

我怎样为动态更新服务和快速替换服务续费？

如果您直接从博威特网络技术（上海）有限公司购买产品：

在动态更新服务和（或）快速替换服务计划到期前，请致电(8621) 54520358或 (8621) 54520368联系博威特网络技术（上海）有限公司并提供有效产品序列号，受理时间为周一至周五的上午9点到下午5点（太平洋标准时间）。

如果您从代理商处购买产品：

在动态更新服务和（或）快速替换服务计划到期前，请联系您的代理商并提供有效产品序列号，您的代理商将安排续费事宜。

如果您还没联系代理商或该代理商不能受理续费事宜，也可以选择直接与博威特网络技术（上海）有限公司联系动态更新和快速替换服务计划续费事宜。

补充条例

上述条例如有改动请见博威特网络技术公司中文网站(<http://www.barracudanetworks.com.cn>) 的最新通知。

附四 梭子鱼垃圾邮件防火墙标准服务条款

为确保客户在购买梭子鱼垃圾邮件防火墙所应该得服务，博威特网络技术（上海）有限公司为客户提供以下标准服务条款：

1. 服务期内垃圾邮件规则库自动动态升级
梭子鱼垃圾邮件防火墙可以设置为每小时或者每日自动通过 Internet 升级，防垃圾邮件及病毒邮件的强大程度与其更新的频度直接相关。
2. 服务期内病毒特征码自动更新
梭子鱼垃圾邮件防火墙可以设置为每小时或者每日自动更新病毒特征代码，提升防御最新病毒入侵的能力。
3. 服务期内免费实时更新垃圾邮件指纹
梭子鱼垃圾邮件防火墙实时更新垃圾邮件指纹检查机制，是大大提升产品对检测垃圾邮件的功能。
4. 服务期内免费实时更新黑名单
梭子鱼垃圾邮件防火墙实时更新黑名单功能，提供强大的动态阻止流行性的垃圾能力。
5. 有限保修：
该有限保修包括原材料和工艺上缺陷。
该有限保修不包括：
外部客观原因如意外事故、滥用、误操作和电源问题
未经博威特网络技有限公司授权私自维修
不按照使用手册使用产品
错误理解博威特网络产品使用手册或错误执行预防性维护
由于使用非博威特网络技术有限公司提供的附件、零件或其他组成部分而引起的问题
产品序列号被遗失或更改
未支付货款的博威特网络产品
6. 服务期内免费电话技术支持支持
(总部)：408-342-5400
(中国)：021-5452-0358
工作时间技术支持（中国）电话：021-54525482
7. 服务期内 Web 网站、电子邮件技术支持
你可以通过以下 E-mail 地址获得技术支持
support@barracudanetworks.com (美国)
support@barracudanetworks.com.cn (中国)

8. 立即更换服务（用户需要购买）

我们了解有时会有一些意外发生，设备也可能出问题所以我们为用户提供立刻更换服务，您只需要支付一份额外的费用。我们就将在您机器损害之后立刻更换您的产品，产品更换时间在美国总部是一天，在大中华地区是三天；这样您可以立即获得产品保障您系统的稳定运行。

博威特网络技术（上海）有限公司
售后服务部