

梭子鱼反垃圾邮件及病毒防火墙对邮件进行扫描过滤，阻止垃圾及病毒邮件进入邮件服务器。一般情况下，该设备安装在防火墙后的内网中或 DMZ 区。物理连接上，应将该设备接入交换机，并分配 IP 地址，就像其他网络设备一样。

## 1

### 安装准备

本向导帮助您一步一步安装梭子鱼。在安装之前，请您务必仔细阅读完本向导，并请做好如下准备：

- 梭子鱼反垃圾邮件及病毒防火墙、电源线。
- 上架导轨 (限 600/800/900 型号)
- VGA 显示器 (推荐)
- PS2 键盘 (推荐)

## 2

### 硬件安装

安装梭子鱼反垃圾邮件及病毒防火墙的步骤是：

1. 将梭子鱼垃圾邮件及病毒防火墙固定在 19 英寸标准机架上或平稳放置。
2. 用网线将梭子鱼垃圾邮件及病毒防火墙背面网络接口连接到网络中的交换机上。
3. 接上标准 VGA 显示器、PS2 键盘及电源线。可以初始化梭子鱼垃圾邮件及病毒防火墙的 IP 设置。**注意：**在刚电源线刚接通的时候，梭子鱼电源将自动打开，几秒后就会自动关闭。梭子鱼非正常断电后再次通电将自动重起设备。但是正常关机后通电，梭子鱼将只自动加电几秒，随后关闭。
4. 按前面板的电源按钮启动梭子鱼。



## 3

### 设置 IP 地址等网络设置

如果连接了显示器，将能观察到梭子鱼的启动过程，启动结束后，在命令行的界面下开始配置：

1. 输入管理员的用户名及密码

- **Login:** admin
- **Password:** admin

```
barracuda login: admin
password:
```

2. 根据您的网络的规划，配置梭子鱼的 IP 地址、掩码、默认网关、首选 DNS 服务器及备用 DNS 服务器。

3. 保存配置。

假如您没接键盘显示器，您可以利用前面板的 RESET 按钮设置 IP 地址。方法是按住 RESET 键一定的时间：（注 1：按住时间达 5 秒时，前面板左边起红黄绿等会闪一下；到 8 秒，12 秒时，也会闪。注 2：并不推荐采用此方法设置 IP 地址。）

IP 地址	按住 RESET 键时长
192.168.200.200	5 秒
192.168.1.200	8 秒
10.1.1.200	12 秒

## 4

### 开放防火墙端口

如果您的梭子鱼安装在企业防火墙之后，您需要开放如下端口：

Port	Direction	TCP	UDP	Usage
25	In/Out	Yes	No	邮件进出、弹回邮件发送。
53	Out	Yes	Yes	DNS
80	Out	Yes	No	病毒、垃圾邮件规则库、系统版本升级
123	Out	No	Yes	NTP

## 5

### 梭子鱼垃圾邮件及病毒防火墙的配置

在梭子鱼所在网络内，找一台电脑，打开浏览器，进行如下配置：

1. 在浏览器地址栏，输入 [http:// 梭子鱼的 IP 地址](http://梭子鱼的IP地址)，加上梭子鱼 Web 管理界面的默认端口 8000。例如：需要管理的梭子鱼的 IP 地址是 192.168.200.200。则在地址栏中应输入：
2. 在登陆界面，输入用户名 admin， 密码 admin。
3. 进入**基础->IP 配置**页：
  - 检查 **IP 地址、子网掩码和缺省网关**是否正确。
  - 输入目标邮件服务器的服务器名/IP，梭子鱼将把过滤好的邮件投递到这里设置的邮件服务器上。例如： mail.<yourdomainname>.com
  - 检查**首选及备用 DNS 服务器**设置是否正确。
  - 输入缺省主机名和缺省域名。梭子鱼弹回信息中将使用这些名称。
  - 在“**允许的收件域**”选项中添加许可的收件人域，除添加好的域之外，梭子鱼将拒绝所有其他域的邮件。收件人域添加完成后，点击**加入**按钮完成添加。

4. 点击**保存修改**保存上述信息。
5. 仅 **100 型号**：进入**用户**页完成下面的一项设置：
  - 在**用户配置**中，输入需要进行垃圾及病毒扫描的用户邮件地址，每行一个，不超过 50 个。
  - 或者选择**启用用户添加**，梭子鱼将在邮件达到后自动的添加邮件用户清单，不超过 50 个，这些用户将得到垃圾及病毒邮件过滤。

**注意：**如果用户没有指定，并且也没有设置自动添加，则梭子鱼将不会对任何进来的邮件作垃圾扫描。
6. 保存修改。

## 6 升级系统版本

进入**高级设置**→**系统升级**。如果有最新的版本，通过如下设置完成升级：

1. 点击**立即下载**按钮，开始下载最新的版本。如需查看下载进度，请点击**刷新**按钮。下载完成后，**刷新**按钮将变成**立即应用**按钮。
2. 点击**立即应用**按钮加载新的版本。这个过程需要几分钟的时间。在下载及更新系统期间，请不要人工关机，避免系统出错。
3. 在新的版本应用后，梭子鱼将自动重启，重启结束后将显示登陆 Web 界面。
4. 重新登陆 Web 管理界面阅读版本通告，了解新版本中改进或增加的功能。

## 7 更改管理员密码

为了避免非法访问，我们强烈推荐用户将默认密码改为更安全的密码。注意，您只能更改 Web 管理界面的密码，不能更改管理控制台的密码。对于用户而言，接上键盘和显示器，可以进入管理控制台，但仅限于修改 IP 设置等有限的操作。

1. 进入 **基本设置**→**系统管**，输入旧密码，并输入新密码。
2. 点击 **保存密码**。

## 8 产品激活

进入**基本设置**→**状态页**，检查本台梭子鱼动态更新功能是否激活。在许可证状态下，确认动态升级功能当前有效。如果动态更新没有激活，请点击其链接登陆到 Barracuda Networks 产品激活页订购并激活升级。

## 9

### 路由邮件到梭子鱼反垃圾邮件及病毒防火墙

为了对邮件进行垃圾及病毒的扫描与过滤，您必须将 Internet 的邮件路由到梭子鱼上，通常有两种方式：

- **端口转发方式**。在防火墙上将 SMTP 25 端口的流量改到梭子鱼反垃圾邮件及病毒防火墙上。这种方式需要对防火墙的端口进行修订，详细地操作请参阅防火墙的操作手册，或咨询防火墙管理员。
- **MX 转发方式**。创建一条梭子鱼的 DNS 记录，将邮件系统的 MX 记录改到梭子鱼的 DNS 记录上。如：

```
barracuda.barracudanetworks.com IN A 66.233.233.88
```

**Example: Modified MX Record**

```
IN MX 10 barracuda.barracudanetworks.com
```

不同的 DNS 管理程序添加相关记录的方法可能不同，但应该与上面的例子相似，其中数字 10 代表了 MX 记录的优先级。**注意：**某些 DNS 服务器缓存信息更新可能需要 7 天，因此可能需要很长的时间邮件才能发到梭子鱼上。

## 10

### 要点

- 如果将外发的流量路由到梭子鱼上，您必须在高级设置—信任转发中进行设置，或者将梭子鱼切换成外发模式。
- 建议您关闭您邮件服务器上的所有反垃圾检查以避免和梭子鱼发生潜在的冲突。

## 11

### 调整梭子鱼的策略

梭子鱼反垃圾邮件及病毒防火墙初始配置将标记多数垃圾邮件，梭子鱼将在这些信的主题上增加提醒如：“[BULK]”。这样，用户可以在自己的邮件客户端如 Outlook 上建立一个特别的文件夹专门接收这些邮件。用户可以进入**基本设置**→**垃圾邮件评分页**自定义评分策略。不过标记分值建议还是用默认值。在您对系统设置比较熟悉后您再根据情况进行调整。

更多的资料，请参考：<http://www.barracuda.com/documentation>。

#### Contact and Copyright Information

Barracuda Networks, Inc. 3175 S. Winchester Blvd, Campbell, CA 95008 USA • phone: 408.342.5400 • fax: 408.342.1061 • [www.barracuda.com](http://www.barracuda.com)  
Copyright 2004-2009© Barracuda Networks, Inc. All rights reserved. Use of this product and this manual is subject to license. Information in this document is subject to change without notice. Barracuda Spam & Virus Firewall is a trademark of Barracuda Networks, Inc. All other brand and product names mentioned in this document are registered trademarks or trademarks of their respective holders. SQS-3410v109-070208-10cn-0407