梭子鱼垃圾邮件防火墙

技术白皮书

公司简介

一. 博威特网络技术公司：

博威特（Barracuda）网络技术公司成立于 2002 年,是提供企业级垃圾邮件解决方案的领导者。在全球屡获殊荣,包括《Network Computing》杂志的编辑选择奖，并于 2004 和 2005 连续获得最佳表现奖。公司的旗舰产品梭子鱼垃圾邮件防火墙系列,为世界各地超过 50， 000 用户提供电子邮件安全防护,包括大量国际知名用户如 Adaptec, Knight Ridder, Caltrans, CBS,乔治亚洲技术学院, IBM,美国国家宇航局, Pizza Hut, Union Pacific `Railroad,和美国财政部等。

博威特网络技术公司在 2005 年 4 月份进一步拓展产品线，增加梭子鱼 Web 安全网关系列，梭子鱼安全负载均衡机系列和梭子鱼应用防火墙系列。这些新品和垃圾邮件防火墙系列一同为各种规模的企业提供完整的应用网络安全整体解决方案。

博威特专业技术服务团队能够提供强大的支援。企业级解决方案广泛适用于大型企业和中小型企业。综合了众多强大功能的梭子鱼产品,兼具易用性和稳定性,赢得了来自客户的广泛赞誉和媒体、评测机构如潮的好评。

二. 博威特网络技术 （上海）有限公司:

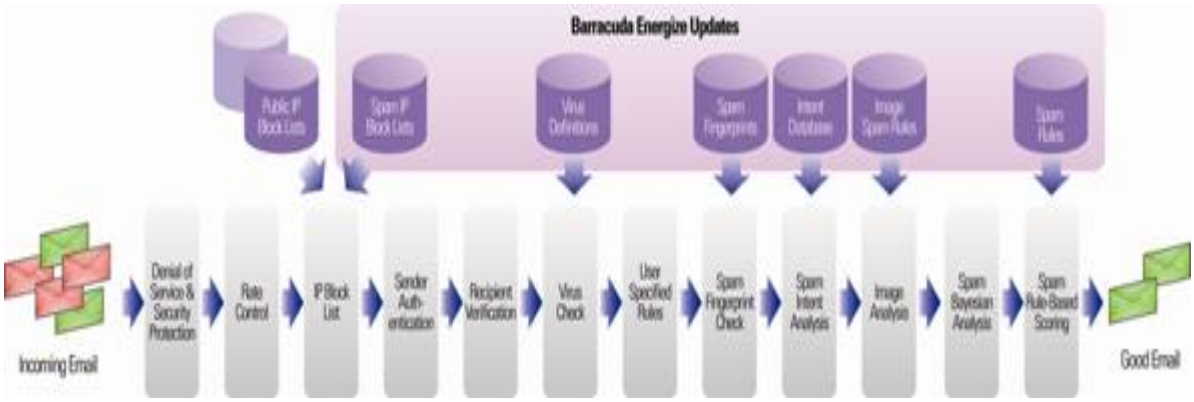
博威特网络技术（上海）有限公司是美国 Barracuda Networks Inc.在中国的全资子公司。在国内，博威特网络技术（上海）有限公司服务于众多企事业单位，其中包括北京宣武区政府，四川电信 IDC，包头钢铁公司，江西党政网 在国内的技术支持中心，专业的技术人员为您提供 24 小时不间断技术支持及产品自动升级服务，并负责产品在国内的汉化工作，以便更好的服务用户。

梭子鱼垃圾邮件防火墙（Barracuda Spam Fireware）提供强大、易于使用、成本效益高的企业级垃圾与病毒邮件解决方案，全球用户数超过 50000 家，是电子邮件安全设备的领导品牌。

梭子鱼（Barracuda）基于业界最坚固的 Linux 内核，并进行了专门的优化；采用自由且功能强大的 Perl 建构了开放稳定的系统内核，具有先进的系统架构，带给用户最轻松的使用体验。安全的 Linux 内核＋健壮的 MTA＋服务器阵列，提供了企业级的容错与负载均衡，能高效、灵活、准确的处理用户企业中的所有邮件。

十分钟！梭子鱼（Barracuda）提供给用户是非常易于使用的产品。用户打开包装箱，把梭子鱼安装在 19 英寸标准机架上，进行简单的配置后梭子鱼立刻开始对企业邮箱提供全面的保护。这一过程仅仅只需要十分钟。梭子鱼（Barracuda）提供给用户的是一种**“即插即忘”式**的产品，无需用户进行复杂的系统操作，管理员通过 WEB 浏览器就可以对设备进行远程的管理，一旦系统调整完毕，管理员无需经常登录系统进行管理，系统运行的各种数据会定时的发送到管理员或相应的每个邮件用户的信箱中。

梭子鱼产品核心设计理念是“垃圾邮件的鸡尾酒疗法”，即采用多种不同的反垃圾邮件技术，对邮件的不同特征进行权方位的检查与过滤；而梭子鱼产品设计架构则采用了分层过滤技术，每个过滤层结合不同的反垃圾邮件技术，多达十二层过滤机制，使辨识率达到 98%。



梭子鱼的 12 层过滤机制，其中 5 层是连接控制过滤（防攻击层、速率控制层、IP 过滤层、发件人认证、收件人检查），7 层邮件内容过滤（病毒检查、用户自定义规则、邮件指纹检查、邮件意图分析检查、图片识别、贝叶斯分析、基于规则评分）。

连接控制过滤

梭子鱼（Barracuda）在连接控制将首先检查 TCP/IP 的合法性以防止 DOS 攻击或其它类型的非法连接：接着将对 SMTP 连接的频率进行统计，防止非法发送者大量的发送垃圾邮件；接着，通过多重 RBL（Realtime Blackhole List）检查核实发件者 IP 地址是否合法。在同类产品中，只有梭子鱼提供多重的 RBL 检测，即梭子鱼公司 RBL 服务器、国际组织 RBL 服务器和用户自定义 RBL 服务器。梭子鱼还率先使用 SPF/微软 Call ID 技术验证发件人的合法性。当然，管理员可以定义自己的 IP 黑名单，拒绝来自这些 IP 地址的连接；梭子鱼提供了 IP 攻击的报表，以方便管理员决策是否将这些 IP 列入黑名单。管理员还可以定义 IP 地址白名单，对来自这些 IP 地址的邮件不进行垃圾检查，但是仍然执行病毒扫描及附件的检查。

梭子鱼（Barracuda）在 SMTP 连接应用层进行五道检查，分别是发件人认证、发件人黑白名单、收件人核实、邮件协议与属性检查和邮件路由。

发件人认证包括两层含义，其一是转发控制，默认情况下，梭子鱼关闭（Open Relay），不会转发邮件；其二如果需要梭子鱼发送邮件，梭子鱼将认证发件人的合法性。认证的方式包括指定转发 IP，指定信任域、指定信任发件人，SMTP 认证，LDAP 认证。

发件人黑白名单针对邮件地址的黑白名单。例如：管理员可以把本公司重要客户的发信人地址列入到白名单，这些邮件将不会进行垃圾检查而快速的通过过滤网关到达用户的邮箱。梭子鱼（Barracuda）还具有几项独特的功能，如**发件人欺骗保护**，这项功能阻止垃圾邮件仿冒用户的邮件域给用户发信。再如，**收件人黑白名单**功能，如公司内部使用的一些邮件群不需要接收外部邮件，此时可以将之加入收件人黑名单中，拒绝外部垃圾信的骚扰。

邮件协议与属性控制连接是否符合邮件协议，检查邮件的大小、每 SMTP 连接的邮件数、连接的时长等信息，避免不合法、长时间占用系统资源或大范围的群发和垃圾邮件攻击。

梭子鱼（Barracuda）支持通过 SMTP 或 LDAP 方式对收件人的地址进行核实，避免垃圾邮件者对服务器发动字典攻击、DHA 攻击，避免邮件服务器接收不存在的收件人邮件，从而较少了数据流，减轻了邮件服务器的负担。

邮件路由包括基于邮件域的路由、基于主机地址的路由、流量控制与延时投递，共同保证正常邮件从网关有控制、有保障的转发到后台邮件服务器。在邮件服务器发生故障时，梭子鱼（Barracuda）将保留邮件 48 小时（默认时间），从而保证邮件服务器发生故障时用户的重要信息不会丢失。

内容过滤

内容过滤是梭子鱼（Barracuda）产品的核心竞争力，梭子鱼通过邮件指纹技术、意图分析技术、图片分析技术、贝叶斯过滤技术、基于规则的评分系统等拦截垃圾邮件，并独创双层病毒扫描引擎对邮件病毒进行高效的扫描。梭子鱼还对附件进行垃圾和病毒扫描。

邮件指纹技术

垃圾邮件发送的商业模型是大规模的发出同样的邮件，通常几天或者几周内甚至几个月内发送数以百万计的邮件，这些邮件虽然可能在细微处有所变化，但是通过特定的算法，却可以将这些邮件的共同特征提取出来。为此，博威特公司设置了大量“蜜罐”，或者说诱骗邮件地址，是用于收集大量的垃圾邮件。再依靠特定的算法，将这些邮件的共同特征——邮件指纹提取出来，形成邮件指纹库。梭子鱼收到邮件后，发送相关的信息到远程的邮件指纹数据库中进行核对，从而迅速的确认这封邮件是否是垃圾。

这种指纹分析的方法和当前反病毒体系中病毒特征码的原理是一样的。在面对一些最新出现的或罕见的垃圾邮件时，它没有多大效用。但是对于哪些大量发送的相同的垃圾邮件，这种方法却具有最高的效率。而且这种方法几乎不会产生误判。梭子鱼（Barracuda）每天更新数百个邮件指纹信息。

意图分析技术

垃圾邮件技术如今变得愈加复杂，许多垃圾邮件变得与正常的邮件几乎一样，在这些邮件中含有 URL 链接，这个链接往往指向一些不健康的网站，或某个商品促销的网站。梭子鱼为此创建了意图分析技术，构建了全球最大、含盖了全球十几个语种的垃圾邮件 URLS 地址数据库。它检查邮件中的 URL 链接，确定邮件是否为垃圾邮件。

该数据库中的不良网址数量已经超过20万，并且每天增加或更新数百个。

图象识别技术（OCR）及 PDF 识别技术

2006 年下半年以来，图象类垃圾邮件的数量越来越多，如下图，梭子鱼采用了 OCR 技术对图片中的文字进行识别，在依据图片规则进行评分。对于特别复杂的图片，梭子鱼还能

将之做成邮件指纹予以判断。2007 年来，PDF 类型的垃圾邮件又迅速增加，梭子鱼有开发了 PDF 识别技术，对 PDF 文件内容进行垃圾邮件评分。

贝叶斯过滤技术

贝叶斯分析：命名于著名数学家托马斯。贝叶斯（1702-1761），他发展了一个数学领域全新的可能性推论理论。贝叶斯分析采用过去事件的知识预测未来事件。

应用到反垃圾邮件领域，贝叶斯过滤与以前收到的垃圾邮件与合法邮件的中相同词语与短语出现的频率对比此邮件中有问题的词语与短语的来确定垃圾邮件的可能性。他能自动适应垃圾邮件变化。是一种动态的智能过滤技术。

贝叶斯过滤器是非常强大的，也是阻断垃圾邮件最为精确的技术。大多数报告显示，当贝叶斯过滤器被“有效培训”以后，过滤器过滤垃圾邮件的准确率达到 99%。为了培训贝叶斯过滤器，需要该收件人大约 200 封有效邮件及 200 封垃圾邮件。在目标收件人中有越多的历史数据库，过滤器越准确。参见 Paul Graham 先生著作的“优化贝叶斯过滤器”http://www.paulgraham.com/better.html。

梭子鱼的贝叶斯过滤技术领先于其它产品，它采用了全新的分词技术，同时支持单字节和双字节语种，需要学习的样本数量更少。贝叶斯能保正系统始终具有较高的过滤率，其它的过滤技术是一种静态的技术，依赖于规则库或特征库的更新。而贝叶斯是智能的技术，他能自动学习新的垃圾邮件，调整自己的字词频度表，使得系统始终维持较高的过滤水准。

采用了分用户贝叶斯后，使得不同邮件用户个性化的需求得以真正的实现。一般反垃圾邮件分用户个性化设置仅限于个人黑白名单。无法满足不同用户对邮件的不同偏好，然而用户通过调整培训自己的分用户贝叶斯数据库，就可以简单的实现这一功能。

基于规则的评分系统

垃圾邮件制造者清楚反垃圾邮件的原理，因此也越来越狡猾，其中常用的一种办法经常将一些单词拼错，“Viagra”可能被有意地拼写为“Vlagra”或者任何一种可能的变体，这样普通的词语过滤器就无法识别。

基于规则的评分系统也被称为人工智能（AI）系统，博威特网络基于海量邮件的分析，定义了近 6000 条垃圾邮件规则，每一条规则对应一定的评分，一封邮件与规则库进行比较，每符合一条规则加上该规则评分，获得的分数越高，该邮件是垃圾邮件的可能性就越高。如果一封邮件超过一定得分门槛（阈值），该邮件将被分类为垃圾邮件。

在这些规则中，可以用来识别变化的词语或短语，例如垃圾邮件引擎侦测到变化型文字，

垃圾邮件引擎会自动回复到原先字词，例如 V.I.A.G.R.A 回复为 VIAGRA。

这些规则不仅包括语义分析，还包括对垃圾邮件发送工具的检测、对邮件中含有图片形态和比重的检测，对于 HTML 格式的各种特征的规则等。通过对一封邮件所有相关的信息都进行相关的智能分析，最终能够准确的判定一封邮件。

由于垃圾邮件发送人及制造垃圾邮件的程序不是静态的，因此博威特持续追踪互联网上的垃圾邮件的变化，及时更新规则库。采用这项技术，可以清除 90%的收到邮件中的垃圾邮件。梭子鱼还专门定义了中文简体、繁体、日语等规则分库，以适应双字节邮件的过滤。

Digital Consultants Computerland	
Digital Consultants ComputerLand	Digital Consultants 公司的总裁兼 CEO Gregory Sirakides 先生说“这个产品易于安装，易学易用，几乎不用配置，很低的维护成本，优秀的价格性能比，博威特垃圾邮件防火墙非常适合我们的客户。”

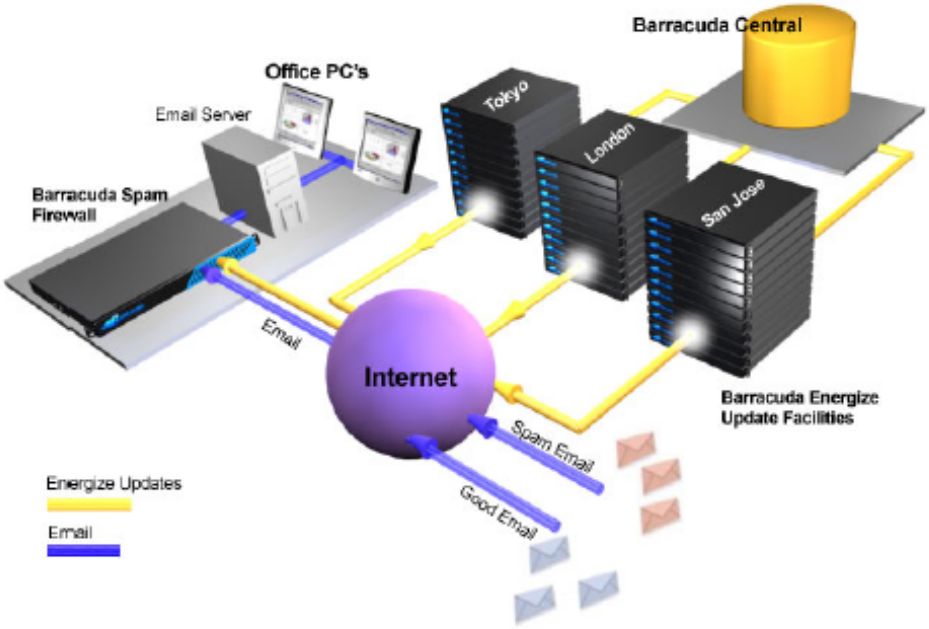
梭子鱼（Barracuda）还提供了丰富强大的自定义过滤策略：用户可以对邮件信头、主题、信体设立阻断、隔离、标记、关键字白名单等不同类型的关键字。再所有检查都进行完毕后，根据用户设立的评分策略，对邮件进行允许、标记、隔离、阻断等操作。梭子鱼（Barracuda）支持完全的正则表达式，为了方便用户使用，梭子鱼公司提供了不同语种的关键字模版。

安全性与易用性

梭子鱼建构在加固的 linux 平台下，去除了不安全的服务，系统运行稳定。管理员可以指定 IP 访问列表，只有列表中的 IP 才能对梭子鱼（Barracuda）进行远程的管理。也可以设置 SNMP 和 API 的 IP 访问列表。并可以通过动态对称的加密的 HTTPs 通道进行。

梭子鱼（Barracuda）支持通过 LDAP 验证收件人地址的合法性，可以避免 DHA 攻击；若用户邮件系统不支持 LDAP，梭子鱼还可以使用 SMTP 方式进行验证。梭子鱼的速率控制机制能够有效的阻止某个 IP 发动的海量邮件攻击。

梭子鱼提供丰富多样的报表，将系统运行的相关数据定时发送到管理员的信箱中，便于管理员及时的了解系统的运行状态。梭子鱼还提供数据库化的日志功能，对每封邮件所做的处理作了详细记录，并且提供了便捷的日志搜索功能，管理员可以方便的查找到所需的日志记录，在必要的时候，日志系统记录的邮件还可以重新进行发送，这样作为邮件系统的备份，保护了数据的安全。



梭子鱼服务的核心—博威特中心

博威特建立了运营支持中心，24 小时在线支持梭子鱼的运行，运行中的梭子鱼将可以自动下载病毒特征代码，垃圾邮件规则库，最新的内核程序。并提供指纹库、黑名单库、意图分析库的实时查询。

梭子鱼（Barracuda）内的所有运行数据均可以备份：包括分用户数据的备份、贝叶斯数据库的备份，系统设置的备份。更可以自动备份数据。此外，电源中断回复后，可自动启动。系统某服务工作不正常时，通过重新启动可自动纠正错误。梭子鱼还提供内核版本“倒车”功能。即如果当前版本发生软件故障，用户可以恢复到上一次正常工作的版本，直至恢复到出厂设置。

个性化定制和个人隐私保护

梭子鱼（Barracuda）是一款国际化的产品，其使用界面可以选择包括中文简体、繁体、英语、日语等在内的九种语言。梭子鱼使用 UTF-8 编码解决了双字节文字（汉语、日语、韩语）在内的各种语言编码的邮件过滤问题。梭子鱼发出的各种报表、通知信息用户均可以定制，也可以选择梭子鱼提供的不同语言通知。

梭子鱼（Barracuda）支持分用户隔离与设置功能，用户将能收到梭子鱼发给用户的隔离邮件的报告，发送报告的时间及报告的语言类型用户均可以自行设定。用户在该邮件中无需登录系统就能对邮件进行相关操作。在登录系统之后，用户可以定义对邮件的处理方式，比如可以选择需要或不需要隔离邮件。可以定义用户自己的黑白名单，通过设定自己的贝叶斯库设定自己对邮件的偏好。可以制定完全个人化的垃圾邮件过滤策略，满足了用户个人性化的需求，同时也有效的减轻了管理员的负担，保护了个人隐私。

关于博威特

Barracuda Networks 成立于 2002 年，公司总部位于美国加州硅谷，是全球提供企业级垃圾邮件解决方案的领导者。在全球屡获殊荣，包括 Network Computing 杂志的 Editor's

Choice Award、Best of Show Award。主要产品 Barracuda SPAM Firewall 系列，为世界各地超过 50,000 个客户提供电子邮件安全防护，销售量稳占全球第一。大量国际知名用户如 Adaptec、Knight Ridder、Caltrans、CBS、乔治亚洲技术学院、IBM、NASA、Pizza Hut、Union Pacific Railroad、和美国财政部等。 Barracuda Networks 的产品有 Barracuda SPAM Firewall、Barracuda Web Filter、Barracuda IM Firewall、Barracuda Load Balancer、Barracuda Message Archiver 等。 Barracuda 专业技术服务团队能够提供强大的支持。企业级解决方案广泛适用于大型企业和中小型企业。综合了众多强大功能的 Barracuda 产品，兼具易用性和稳定性，赢得了来自客户的广泛赞誉和媒体、评测机构如潮的好评。目前产品销售遍及全球 80 个国家，并于各地设立分公司和经销商体系。