

# 邮件过滤网关 (KShield Gateway)

## 反垃圾邮件技术白皮书

Writer: Alicia Peng

CA-JinChen R&D  
Tuesday, Nov 23, 2002

# 目录

1. Copy Rights .....	3
2. 阅读对象.....	3
3. 反垃圾邮件技术.....	3
4. 网关过滤工作原理.....	4
5. 垃圾邮件过滤原理.....	5
6. 垃圾邮件过滤引擎适用范围.....	7

# 1. Copy Rights

本篇材料是冠群金辰产品 KShield Gateway 系统的技术白皮书。该文档属于冠群金辰软件公司 ( CA-JinChen Software Co.,Ltd. )。未经本公司授权,不得以任何目的对本文档的整体或部分进行分发、复制或引用。如果使用该文档,必须表明文档出处和版权信息。

版权 (c) 1998-2003 , CA-JinChen Software Co.,Ltd 保留所有权利。

## 2. 阅读对象

本文详细阐述了冠群金辰公司 KShield Gateway 系统的反垃圾邮件引擎的实现技术,主要供技术人员参阅以便选择合适的反垃圾邮件产品。关于产品对邮件病毒的检测原理,请参考 KShield Gateway 系统的另一篇白皮书。

## 3. 反垃圾邮件技术

随着因特网的不断普及,国内的用户数呈指数级增长。其中电子邮件是 Internet 所有服务中最基本的服务,超过百分之八十的用户使用电子邮件服务。它为人们的工作、生活、娱乐提供了极大的便利。在充分享受电子邮件带来的便捷、实时和廉价的同时,网络时代的人们也饱尝垃圾邮件带来的烦恼。几乎每个人的信箱都充斥着大量来历不明的邮件,垃圾邮件像瘟疫一样蔓延、污染网络环境,影响网络的正常通信。而在我国,由于成百上千的开放邮件中继服务器被国外不法分子利用,国外许多邮件服务商曾一度封杀了中国邮件服务器的 IP 地址,致使中国用户蒙受不可估量的损失。

垃圾邮件的内容形形色色,主要包括以下几种类型:

- 1) 推销产品。向用户宣传自己的产品或者服务,这类信件最为常见,占 80%左右;
- 2) 恶意骚扰。不停地向特定的邮箱发送信件,使你的信箱被填满而无法接收新的信件,从而扰乱正常工作的信息交流,这种情况大约占 5%;
- 3) 政治,色情等宣传。例如“大参考”等反动政治刊物和一些色情内容信件,占 10%;
- 4) 其他一些来历不明的信件。

垃圾邮件给邮箱用户以及邮箱供应商都带了麻烦以及经济损失。曾经发生过由于通过中国一些 IP 地址发出的垃圾邮件泛滥,导致中国电子邮件被欧美封杀的情况。同时,大量的反动的、色情的垃圾邮件给青少年带来的却是身心的损害,贻误下一代。

垃圾邮件问题已引起有关方面的重视,不久前,中国互联网协会公布了对“垃圾邮件”的正式定义:1、收件人事先没有提出要求或者同意接收的广告、电子刊物、各种形式的宣传品等宣传性质的电子邮件;2、收件人无法拒收的电子邮件;3、隐藏发件人身份、地址、

标题等信息的电子邮件；4、含有虚假的信息源、发件人、路由等信息的电子邮件。可见垃圾邮件问题已越来越严重，应采取相应措施减少垃圾邮件，维护电子邮件的正常使用。很多大型邮件服务商都付出了大量的人力和物力来试图消除垃圾邮件，但垃圾邮件却始终屡禁不止。

垃圾邮件数量的增长速度如此之快的原因在于，第一，垃圾邮件一直被吹捧为是一种最有效却最廉价的广告形式。邮件地址列表很容易买到，也很容易从英特网搜集，特别是为了工作的需要，企业一般都在 Web 站点列出了员工的电子邮件地址。这使得编辑一个邮件地址数据库变得非常的廉价和容易。然后，再使用一个廉价的邮件软件按数据库中的邮件地址自动发送出去即可，非常简单。其次，传统的控制方法无法有效地过滤垃圾邮件，使得终端用户经常收到来自不同地方的商业广告。垃圾邮件制造者是通过邮件报头欺骗，对邮件主题和内容进行处理以及利用第三方服务器进行转发来达到目的。一个常见的垃圾邮件伪装方法是利用网络中的开放式 SMTP 服务器进行转发。如果网络中的一台 SMTP 服务器没有被配置为禁止转发电子邮件，那么它将可能成为被垃圾邮件制造者利用的对象。

在使用垃圾邮件过滤产品之前，用户只能通过设置自己的邮件客户端来过滤一些垃圾邮件，如在 Outlook Express 中设置规则，对收件人、发件人、邮件主题、正文、附件名、邮件大小做一些限制。但是，由于操作的相对复杂度，事实上很多用户没有做任何配置。加之很多企业邮件服务器没有对邮件转发做任何限制，导致企业用户每天收到大量垃圾邮件，或大量垃圾邮件通过这些企业的邮件服务器发送出去，甚至导致邮件服务器的“拒绝服务”。

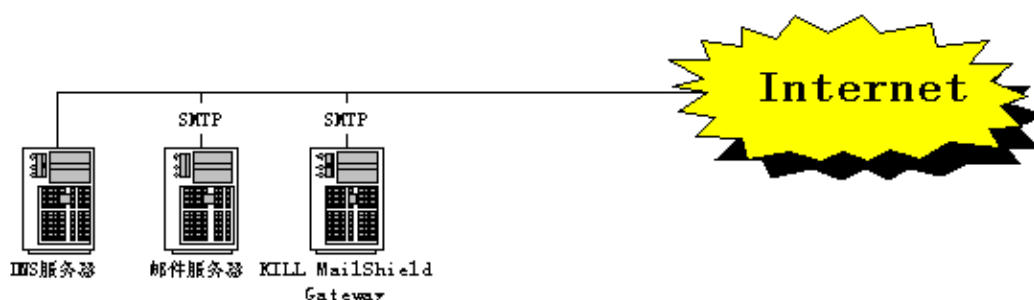
要想在这场对抗中获得主动，我们的眼光自然移到了企业的网络边缘上，在大门口挡住垃圾邮件。这种想法衍生出我们的邮件过滤网关—KShield Gateway 的垃圾邮件过滤引擎。关于其邮件防病毒引擎可以参考冠群金辰的另外一篇白皮书。对于在网络边缘防范垃圾邮件，一个自然的想法是在邮件服务器上安装反垃圾邮件引擎，检查进出该邮件服务器的邮件。可是由于该任务的引入，使得本来负荷就不轻的邮件服务器必须分出宝贵的系统资源用来支持垃圾邮件过滤引擎的工作；这对于小规模邮件系统是可行的，对于大容量（用户数）的邮件系统会造成相当程度的延时，甚至漏收漏发邮件。另外，当前的邮件系统也有很多种，如 Notes、Exchange、Sendmail、Qmail、Postfix 都有相当的使用用户。如果要使用反垃圾邮件软件，不同类型的邮件服务器需要不同的软件，如果用户升级了邮件系统的版本或改用了另外一种邮件系统，通常需要重新升级或购买相应的软件，同时，邮件系统是企业网络的核心服务器，在核心服务器上安装和卸载软件都是有相当风险的。

KShield Gateway 使用一种与邮件系统类型无关的新技术来检查进出邮件，下面我们详细阐述。

## 4. 网关过滤工作原理

KShield Gateway 是一个针对 EMAIL 系统的 SMTP 协议进行过滤的产品。因此 KShield Gateway 的应用只与是否使用 SMTP 协议有关，而与具体的邮件系统无关。KShield Gateway 包括邮件病毒过滤、垃圾邮件过滤、敏感信息过滤等引擎，根据用户需要可进行功能扩展。在性能上，由于 KShield Gateway 使用独立的硬件平台，工作效率要远远高于在邮件服务器上直接安装过滤软件的方式。同时，用户还可以通过均衡和集群的使用线性地扩大 KShield Gateway 的处理能力。在对 SMTP 协议的支持上，当前 KShield Gateway 支持标准的 SMTP 和 SMTP 的扩展协议---ESMTP。

对于发进来的邮件，KShield Gateway 主要是利用邮件路由协议的特点进行工作，出于容错和扩展方面的考虑，简单邮件传输协议(SMTP)在设计时引入了邮件路由的思想，邮件总是首先试图传递给优先级值相对较高的 MX 邮件服务器，失败后才试图传递给优先级稍低的 MX 邮件服务器；同时邮件总是在试遍了同一优先级的 MX 邮件服务器都失败后，才试图传递给优先级稍低的 MX 邮件服务器。因此一封具有一个收件人地址的 Email 可以有多个 MX 邮件服务器目标，每台 MX 邮件服务器可以设置成不同的优先级，高优先级的邮件服务器将先进行处理，如果高优先级的邮件服务器出现意外，邮件会自动发向第二优先服务器，依次直到最低优先级服务器。在使用中，我们赋予 KShield Gateway 最高的优先级，KShield Gateway 具有完整的 MTA 服务功能 这样所有的邮件将先发到 KShield Gateway，进行处理，再由 KShield Gateway 通过 SMTP 协议传给 MX 邮件服务器。KShield Gateway 典型的接入方式如下图：



**注：邮件服务器的优先级在 DNS 服务器中设置。**

对于发出去的邮件，可以在 DNS 中修改 RELAY 服务器(即发件服务器)的 IP 指向，或者用户直接修改自己所用的邮件客户端软件的 RELAY 服务器以指向 KShield Gateway 就可以了。

显然，这种方式规避了在邮件服务器上直接安装邮件过滤软件带来的问题，它与具体使用的邮件服务器类型无关，无需占用邮件服务器的系统资源，相比在邮件服务器上安装过滤软件而言，具有更高的工作效率。它的接入方式也很简单，通常无须修改邮件服务器的任何配置，即使用户更换了新的邮件服务器，也无需更换 KShield Gateway，保护了用户的已有投资。同时，KShield Gateway 具有很好的伸缩性和扩展性，当一台 KShield Gateway 不够用时，用户可以简单地再增加一台 KShield Gateway 进行扩充，如果使用集群模块，还可以做成 KShield Gateway 集群，实现统一管理。KShield Gateway 使用了多种技术，最大限度地保证了与各种邮件系统平滑地结合，以及认证、队列和负载的处理。

当然，每种技术都不是十全十美的，KShield Gateway 也不例外。首先，它只支持对 SMTP 协议的邮件过滤，另外用户需要给每台 KShield Gateway 一个 public IP。

## 5. 垃圾邮件过滤原理

前面介绍了邮件过滤网关 KShield Gateway 的工作原理和垃圾邮件的特征，下面介绍其垃圾邮件过滤引擎的工作原理，可以看到 KShield Gateway 的垃圾邮件过滤引擎从各个方面进行检查，切断垃圾邮件的源头，可有效防止未授权的邮件进入或发出，阻挡垃圾邮件、禁止邮件转发和防止电子邮件炸弹。它通过消除不需要的邮件，有效降低网络资源浪费，与 KShield Gateway 的病毒过滤引擎一起，确保企业邮件服务器不受垃圾、病毒邮件的干扰。

## 一、采用 SMTP 转发认证

SMTP 认证是针对无限制转发采取的措施。所谓无限制转发，就是任何人都可以使用你的服务器发送邮件，一方面隐藏了真实的来源，另一方面转移了资源成本：发送者可以使用一台简单的 PC 机借用你的强大的服务器一次发送几十万封信。OPEN RELAY 是由于历史的原因---电子邮件使用的发信协议 SMTP（简单邮件传输协议）不需要进行任何身份验证导致的邮件服务器的安全缺陷，虽然目前绝大多数邮件服务器都具有关闭或限制 OPEN RELAY 的功能，（有的需要更新到某个版本之后，有的需要打补丁。）但仍有很多企业没有对邮件转发做任何限制，导致大量垃圾邮件通过邮件服务器转发。

为此，如果用户的 RELAY 邮件服务器要求 MUA 进行认证，在引入了 KShield Gateway 之后，SMTP 认证的过程将由 KShield Gateway 来进行。KShield Gateway 会将这一认证过程的数据流重新定向给用户的 RELAY 邮件服务器，并根据认证的结果来决定是否接收 MUA 的发信请求。认证的过程完全遵循 ESMTP 的认证协议标准。

如果用户的 RELAY 邮件服务器不支持 SMTP 认证，可以使用 KShield Gateway 的 SMTP 认证扩展模块，KShield Gateway 有 POP3 用户和 Windows 域用户的 SMTP 认证扩展模块，可以将 SMTP 认证协议转变为对 POP3 用户或对 Windows 域用户的认证协议，这样用户就可以使用 KShield Gateway 进行发信认证了。增加了 SMTP 认证功能后可确保只有授权用户才可以使用企业的邮件服务器，大大减少了垃圾邮件的来源。

## 二、自定义垃圾邮件过滤策略

KShield Gateway 的垃圾邮件过滤引擎支持用户根据邮件的下述信息过滤相关邮件：

1. 可以针对信件的主题、信件地址和信件正文、附件名称、收发件人等进行关键字过滤。如信件中包含“促销”“法轮功”等字样。
2. 可以拒收来自某个 IP 或者网段、域的邮件。
3. 可以限制系统总的收信进程数。
4. 可以限制对任意 IP 的连接数。
5. 可以限制一封信总的收件人的数目。
6. 可以限制每封信的大小。
7. 可以自定义垃圾邮件列表，阻塞来自列表中地址发来的邮件。

## 三、采用第三方垃圾邮件列表

KShield Gateway 支持全球最大的反垃圾邮件组织 MAPS（Mail Abuse Prevention System）提供的 anti-Spam 数据库，包括 RBL（Real Time Black-hole list）、DUL、RSS 以及 RBL+等，有助于减少对网关的大量邮件的恶意攻击。

综上所述，KShield Gateway 强大的抗冲击力能力和完善的过滤功能，使您的邮件系统在这个有害信息和垃圾邮件充斥的 Internet 中给用户和管理员一份安心。

## 6. 垃圾邮件过滤引擎适用范围

1. 大型邮件服务提供商，比如 ISP/ICP 所提供的主机托管、信箱托管、免费邮件或收费信箱服务等等。
2. 企业提供的邮件服务。
3. 学校提供的邮件服务，比如在主流 UNIX 操作系统上流行的邮件服务器，Sendmail、Qmail、eYou Mail 等等。
4. 政府职能部门的邮件服务等。