金笛电子邮件系统

反病毒反垃圾方案

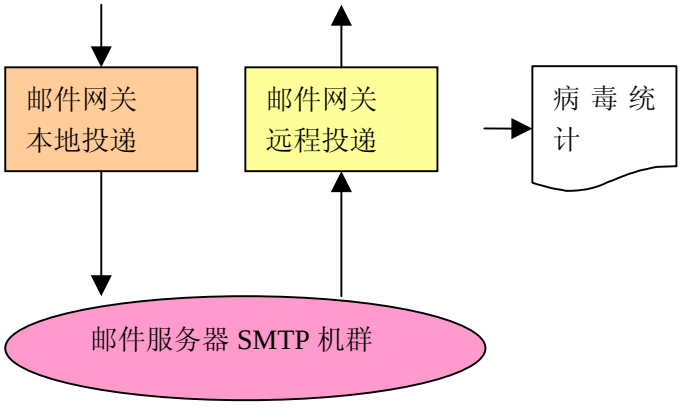
金笛电子邮件系统与反病毒厂商合作，为用户提供更多功能、高性能的邮件防病毒方案。	
KASPERSKY lab	俄罗斯知名反病毒厂商 kaspersky，杀毒效率高，linux/unix 下杀毒效果出色，目前 163 使用的就是此款杀毒软件。
TREND MICRO 趋势科技	世界知名的防病毒厂商，其邮件病毒防火墙可以直接监控 smtp,pop,http,ftp 端口，查杀进出端口的病毒。优点是自动升级，自动更新病毒码，无需人工干预；缺点是价格较贵。
CLAMAV	一款 OPENSOURCE 开源软件，在 linux 平台有很好的性能表现。病毒特征库更新升级比较快。

目录

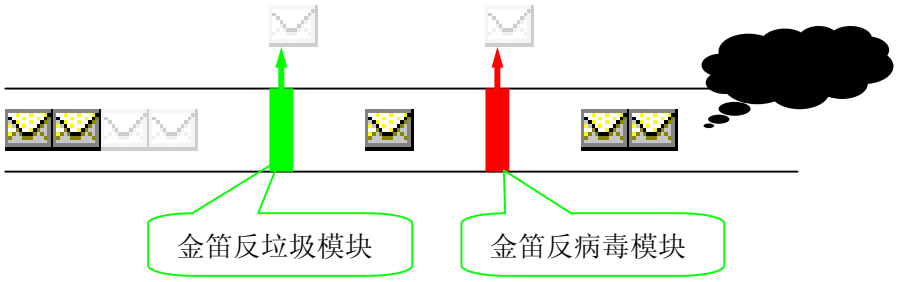
一、应用模式

金笛电子邮件系统反病毒、反垃圾邮件应用模式：

1．系统前端放置邮件网关（适合 20－50 万用户）
架构图



2．系统内嵌防病毒、反垃圾邮件模块（适合 50－100 万用户）



3．网页在线杀毒（适合 100 万以上用户）
　　在收发邮件的页面，嵌入杀毒功能，可以由用户手动杀毒。这种方式将杀毒过程分散，因此可以支持 100 万以上的用户邮箱。

二、推荐方案

　　推荐采用反病毒模式 1 或者反病毒模式 2。

三、金笛防病毒、反垃圾邮件技术特色

金笛®邮件系统的反垃圾、反病毒产品是春笛公司多年的技术结晶。综合运用动态黑名单、 静态黑名单、IP 阻断、DNS 反向解析、邮件打分、bayes 特征库、Razor 国际反垃圾协作网等技术手段，垃圾邮件的识别率高达 95%-98%。病毒邮件的识别率也在 95%以上，可以查杀 20000 多种病毒，对于目前比较流行的邮件病毒 sobig, netsky, mydoom, Worm.SomeFool.Gen 有 100%的免疫力。春笛公司与多家知名防毒厂商合作，支持病毒特征库定时在线升级，保证升级频率一周 3 次以上。

金笛邮件设计成傻瓜化、智能化，不需要复杂的配置，最大程度降低学习和维护的成本。

一、防毒功能特点

1. 采用先进的技术架构，绝大部分操作在内存处理，峰值处理能力为 18 万封/小时，比普通的反垃圾邮件网关快 10 倍以上。

2. 彻底查杀隐藏在 zip/rar/tar.gz 等压缩文件中的病毒，深度可达 20 层。

3. 发现病毒邮件后，金笛®邮件系统可以根据系统设置决定是否通知发信人(sender),收信人(recips)，管理员(admin) 中的一位或者多位. 报警通知邮件采用中英文 2 种提示,用户也可以自己定制提示信息。

4. 病毒特征库的升级频率可以从 10 分钟-1 周可调，每次升级都有详细的 log 日志，自动发送到管理员的邮箱. log 日志可以设定大小,自动回滚使用。

5. 金笛®邮件系统内置的杀毒引擎支持多线程(最多 10 线程),支持 15 层目录深度搜索扫描，支持防病毒系统自检功能,开启自检功能后,防毒系统每隔 1 小时会自检一次。

6. 支持病毒邮件短信 SMS 报警通知功能。

7. 病毒特征库升级通过由升级服务进程自动完成,升级时通过 DNS 轮寻,连接最快的升级服务器. 1 次升级失败时,系统自动重试 9 次。

二、防垃圾邮件功能特点:4 层垃圾邮件防护

第一层: 网络层采用 IP 阻断和动态黑名单

在网络层,金笛®邮件可以设置屏蔽任何一个 IP,一个网段;也可以屏蔽任何一个发信人,一个域。动态黑名单采用黑洞技术,可以实时获取反垃圾邮件列表。金笛邮件网关支持由国际反垃圾邮件组织提供的实时黑名单 RBL，系统预设 bl.spamcop.net, sbl-xbl.spamhaus.org 两个黑名单列表。

第二层: smtp 协议会话格式检查,DNS 反向解析

在这一层,金笛邮件网关在 SMTP 协议的每个阶段进行判断：MAIL/FROM/RCPT/DATA，对于不符合 RFC 规范的邮件，都作为垃圾邮件处理. 对于不能正确反向解析的,也作为垃圾邮件处理。

第三层: 动态白名单

如果某一个发信人发送的邮件均为正常邮件,积累到一定数量后,系统自动将发信人加入白名单列表。

第四层: 基于 Bayes 算法的内容过滤

通过内置的贝叶斯(Bayes)库对进入邮件系统的每封邮件的头部和正文进行分析,得出阀值,阀值低于 5,则为正常邮件;如果超过 5,金笛邮件网关判定为垃圾邮件,会在主题增加 SPAM***字样;如果阀值超过 7,系统会自动归置垃圾邮件;阀值超过 9,系统会自动删除. 对于主题带有 SPAM 标记的邮件,用户可以通过客户端软件或者 webmail 设置过滤规则转存到一个文件夹,定期检查,确认无误后删除。

四、各反病毒引擎功能和性能比较

俄罗斯反病毒专家- Kaspersky

Kaspersky 提供了一个广泛的抗病毒解决方案。它提供了所有类型的抗病毒防护：抗病毒扫描仪，监控器，行为阻段和完全检验。它支持几乎是所有的普通操作系统、e-mail 通路和防火墙。Kaspersky 控制所有可能的病毒进入端口，它强大的功能和局部灵活性以及网络管理工具为自动信息搜索、中央安装和病毒防护控制提供最大的便利和最少的时间来建构你的抗病毒分离墙。

Kaspersky 抗病毒软件有许多国际研究机构、中立测试实验室和 IT 出版机构的证书，确认了 Kaspersky 具有汇集行业最高水准的突出品质。

目前 163 电子邮局在线杀毒用的就是 kaspersky 的引擎。

关于kaspersky的更多介绍：http://www.kaspersky.com/

产品特点：

1.整合性网际安全保护

InterScan VirusWall 提供网络入门网关高效能的三合一防护功能；防止电脑病毒以及恶性程序的入侵。可选择搭配 eManager 电子邮件安全管理模组，提供垃圾邮件以及邮件内容过滤的功能，同时还可控制邮件收发的时机。

2. 即时病毒检测与清除，在网关口拦截 Internet 从 SMTP、HTTP、以及 FTP 渠道进入的病毒
3. 与 FireWall-1 以及其他主要品牌的防火墙 100%兼容
4. 自动更新病毒代码
5. 可通过 Windows 介面程序管理，或者是通过网页浏览器从远端控管
6.支持 Check Point Software Technologies 的 CVP 标准(Solaris 以及 Windows NT, Intel 平台)
7. 可选择设定将恶性的 Java 以及 ActiveX 程序在网关口拦截下来
8. 通过趋势科技与 Lucent 共同研发的内容扫描协定，可与 Lucent 的 Managed Firewall 直接整合(Solaris 以及 Windows NT, Intel 平台)
9. 可选择搭配 eManager 电子邮件安全管理模组
过滤垃圾邮件以及不当内容邮件，同时控制邮件发送的时间 (仅支持 Windows NT, Intel)
10. 可选择搭配 Y2K Scanner 互联网 Y2K 过滤测模组
检查进出邮件的附件内容是否都已经修正为符合 Y2K 标准年序的格式。(仅支持 Windows NT, Intel)

技术优势：

interScan 与 Jindi-Mail 通过 SMTP Forward 实时检测过滤进出邮件服务器的电子邮件附件是否挟带病毒。

趋势科技专利的扫描引擎：

InterScan VirusWall 采用趋势科技多线程 (multi-threaded) 执行的 32 位元扫描引擎来检测成千上万的病毒，百分之百检测 Joe Well s Wild List 所列出在外流行的电脑病毒。此外 InterScan 还可检测到一些未知的病毒，同时还支持 16 种以上的压缩编码格式，而且可扫描多达 20 层的重复压缩文件。

自动更新病毒代码：

InterScan VirusWall 可以定期自动到趋势网站更新，不必用户手动更新。此外，必要时候，趋势科技还会提供紧急的病毒代码更新服务。

完整而容易管理的 log 日志

InterScan VirusWall 随时有完整的活动纪录档，详细记载每一只拦截到的病毒以及每一件可疑的入侵事件：包括档案来源、名称、收件人、收到日期、病毒名称、以及所采取的处理行动。让管理员很容易找出问题的来源，采取适当的反应。

弹性的设定与通过 Internet 来管理的方式

InterScan VirusWall 在检测到病毒或入侵活动时，可以采取下列任何一项或多项的措施： a 警示系统管理人员 b 隔离中毒文件，等待后续的清除或处理 c 删除中毒文件 。在严格的管制条件下，与许用户下载该文件 InterScan VirusWall 包含 Windows 介面以及通过 ISAPI/CGI 网页浏览器的设定介面，提供最佳的管理弹性。

最低系统需求：

Solaris: Solaris 2.5 或更高版本，256 MB RAM，6 GB 硬盘空间做置换档

Linux: Red Hat Linux 6.0 或更高版本，Pentium II 350 或更快 CPU，256 MB RAM，2GB 硬盘空间。

关于趋势科技的邮件防病毒产品的更多介绍，请登陆http://www.trendmicro.com.cn