

**Sherlock**  
侠络客邮件安全  
全方位解决方案书

## 目录

概述 .....	3
侠络客系列产品提供的解决方案 .....	6
产品主要特性和优点 .....	7
实际应用的常用网络架构 .....	9
1. 基本架构.....	9
2. 数据库独立架构.....	10
3. 进出分离架构.....	11
网桥模式.....	12
案例说明 .....	13

## 概述

在现代社会中，电子邮件已经成为了一种重要的通讯手段。随着因特网的不断发展，它在工作中的使用地位会越来越高。替代传真、信件等传统的通讯方式成为必然。

根据调查显示，现在全世界每天传递的电子邮件在 200 亿以上。大部分公司都通过邮件的方式，进行商务沟通和业务的协同工作。公司对于邮件的依赖性越来越强烈，但是随着邮件使用频率越来越高，其相关的管理问题也就凸现出来。主要问题包括以下内容：

1. 邮件泄密：由于邮件中，可以携带任意附件进行传递。这样就存在了通过邮件的方式把公司内部的机密文件或者图纸资料泄漏出去，不但影响公司的利益甚至关系到公司的存亡。
2. 邮件病毒：现代病毒的传递已经以邮件方式作为主要传递途径了。而且感染攻击性很强，对于以往的单机防毒体系做出了很大的挑战，往往一台主机的防毒功能没有更新，导致整个网络中交叉感染病毒，杀之不尽。而邮件服务器则可能成为了病毒的温床和避难所。
3. 垃圾邮件：据调查显示，每天垃圾邮件的数量已经超过了正常业务邮件的数量，而且此趋势还在不断的增长。对公司的带宽资源和日常工作效率同时受到影响。
4. 邮件服务器被黑客攻击：现在黑客攻击网络服务器的事件越来越频繁，对公司的正常业务的威胁越来越大。一旦出现黑客毁坏公司邮件服务器的状况出现，直接导致公司邮件服务的中止和邮件服务器上的邮件被丢失，而且要恢复原来的邮件服务状态也是很困难的。这对企业的运营的损失是非常巨大的。
5. 邮件资料丢失：一般公司员工浏览邮件使用的是 pop3 的方式，把邮件从服务器上下载到本地客户端进行查看。这样当某一个员工机器出现意外情况导致数据丢失，他的邮件也会丢失，这些邮件可能包含了一些客户的来往资料和联络方式等等，或者当该员工离职后，删除他主机中的邮件资料，公司也就可能失去了一些客户信息，从而影响了公司的业务和相关利益。
6. 邮件资源非正常使用：公司员工利用公司的账号做私人用途或者用于非工作性质的邮件传递。往往利用邮件传递一些图片文件，各种笑话，甚至用来传递电影之类的东西。严重增加了公司邮件服务器的负担和带宽资源的占用。即使不断增加网络资源也始终无法根本解决问题，甚至威胁到邮件服务器运作的稳定性。

针对以上公司对邮件管理的问题，企业对于邮件管理提出了以下需求：

1. 法律责任：如何避免由于员工的不正当邮件导致企业受到连带的法律责任。
2. 安全考虑：如何防止公司的机密文件不被从邮件系统泄密
3. 工作效率：如何避免由于员工利用公务时间处理私人邮件和垃圾邮件导致工作效率的降低。
4. 法律和审查机制：当出现法律纠纷的情况，是否可以提供有利的证据，或者给政府相关部门提供有效的数据。
5. 信息的共享：能否让一些有利公司和部门的成长的资料能够及时共享，提高员工的技能和业务水平，做到真正的知识管理。

我们分别从“提高生产效率”，“信息安全防护”和“邮件信息保存”三个方面来讨论：

#### 提高生产效率

对于企业来说，电子邮件、网络系统和计算机设备的投资是用以「生财」的工具，员工当然不应该挪为己用，甚至因为上网行为降低工作效率。另一方面，大量的邮件数据散布在众多员工的终端计算机内，邮件内容若不慎损毁将造成公司生产力，甚至资产的直接损失。

根据 Gartner Group 所发布的调查报告，企业员工每天花在处理邮件的时间将近一个小时。以每天工作八小时计算，邮件系统可能占全企业生产力的 1/8；这也和 Ferris Research 所提出的另一份报告相符，这份数据指出邮件系统可以贡献企业生产力的 15%到 20%。从另一个角度看，员工处理非关公司业务的邮件，当然也相对地减弱本来预期的生产力。不幸的是，有高达 76%企业员工承认利用公务时间收发私人邮件。

要降低员工对邮件系统公为私用，通过适当的监控机制进行内容审查是最有效的方法。邮件监控首要在于阻吓和宣告，企业应当先制定邮件使用管理办法，再基于此办法建立监控机制，并公布让所有员工了解监控的目的和方法。企业一旦实施监控办法，可以很有效地阻吓非公务性和不适当的邮件。调查资料证明 75%的企业认为：适当的网络监控机制可以有效减少员工私用网络资源，进而提升 IT 系统的生产力。

此外，企业每日进出的邮件不断累积，无形中就产生含有丰富信息的知识库。过去由于缺乏总体的管理和整理的工具，邮件的知识资产无法被有效利用。如果对邮件适当的管理和共享数据，邮件对企业的贡献度更多，也能创造更大的生产力。例如，从各员工和客户往来的历史邮件中，去追踪相关项目的

来龙去脉，更深入掌握项目状况和评估绩效。再如，客户服务部门可以借助邮件管理系统，自动搜集和客户互动的邮件，不断累积技术问题知识库。

## 信息安全防护

邮件渐渐变成业务主要工具之后，公司内部将逐渐走向“无纸化”的工作环境，重要的业务信息不再以信件、传真或其它传统方式进行，而是用电子邮件系统取代之。电子邮件数据散布在公司各角落，如果没有妥善的备份和管理机制，即有可能因为计算机故障而毁损；更甚者，应该属于公司的邮件信息资产也可能在员工离职后荡然无存。这些邮件资产的危害，对公司生产力和竞争力的伤害更大，也同时违背信息“可用性”的安全目标。

因此，企业对于邮件资产的管理应该和纸张文件一样，具备“可保管”、“可追踪”、“能交接”等管理特性。基于储存空间的考量，一般 POP3 服务器并不永久保存所有邮件；邮件一旦被下载之后，个人计算机才是最终的储存点。要达到邮件资产管理的目的，唯有利用中央式邮件备份系统才能实现。只要企业能把所有网络上往来的邮件立即而确实地备份下来，自然不怕个人计算机端邮件的毁损或遗失。

再者，对于信息安全首要目标：“机密性”来说，电子邮件是最方便的泄密管道。邮件系统容易操作，可在同一时间传送给众多收信者，一旦泄密就无法收拾(往往是人为失误)。若是使用 Bcc (密件副本)功能，收件者更无法得知原信究竟拷贝给了多少人！

## 邮件信息保存

长期以来，一般企业解决邮件管理的手段除了制定管理办法之外，在技术上大多采用软件对进出邮件进行关键词的检查和过滤；也就是事前的防范措施。然而往往对于关键词设定上精度和广度的局限，不能达到完全阻拦不当邮件的效果。许多邮件过滤技术的研究者指出：关键词的过滤条件设定对用户而言极其困难，不适当的过滤条件不但无效而且很可能造成严重的问题。不当邮件被漏掉并放行之后，管理者完全不知其去向，也就只能闭起眼睛任其翱翔四海了。

当事前过滤无法奏效时，企业仍应保有事后应变的能力，包括：尽早发现和检查不当邮件内容，以及避免不当邮件为企业带来法律责任。在 AMA 的调查报告指出，将近 8.3 % 的美国企业曾经因为员工所寄发的性骚扰或性别歧视邮件而接到法院传票。随着企业对邮件系统的依赖日深，企业应该赶快建立起搜集和储存邮件的机制，以备未来作为证据之用。

电子邮件在法庭上是否可以作为直接证据，尚待法界人士继续讨论。但邮件在调查阶段的可用性早已获得各国法律界承认和重视。在微软反托拉斯法控诉当中，比尔盖兹所寄发的电子邮件内容就被美国司法部作为违法事实的左证，并成为邮件证据的知名案例。

## 侠络客系列产品提供的解决方案

针对以上公司对邮件管理的问题和需求，侠络客系列邮件安全产品提供了良好的解决方案。

侠络客系列邮件安全产品是针对邮件的各种问题提供相应的解决方案。而且为了满足不同的客户需求，细分为三个产品来为客户提供不同方面的产品介绍。它们分别为

- 侠络客邮件备份追踪系统 **MailSherlock**
- 侠络客反垃圾邮件过滤系统 **SpamSherlock**
- 侠络客病毒防护系统 **VirusSherlock**

其中 MailSherlock 是一个邮件监控备份管理软件，通过 SMTP 转发方式，记录所有进出的邮件，并且提供邮件网关模式保护，垃圾邮件阻挡，阻止拒绝服务攻击 DoS，邮件备份，邮件统计，邮件过滤，层级管理和防病毒功能。为企业的邮件服务提供的有效的控管和保护机制，降低了公司信息泄密的风险。

SpamSherlock 则主要针对垃圾邮件提供专门产品，去除了 MailSherlock 的邮件备份功能，而完全针对垃圾邮件提供多种反垃圾邮件监控机制。包括黑白名单，DNS 反查，国际 RBL 过滤，邮件帐号检测，邮件内容评分过滤机制等等。同时提供个人化的反垃圾邮件设定机制，可以让员工根据自己的实际情况设定垃圾邮件的过滤规则和过滤内容，从而提高整体的反垃圾邮件能力。

VirusSherlock 是针对邮件病毒提出的解决方案，除了邮件病毒外，还能够作为网关防毒设备。因为 VirusSherlock 可以对 HTTP, FTP, POP3, SMTP 四种端口进行病毒扫描，强化整体防病毒体系，对中小型企业和特定部门提供网络防毒杀毒功能，并且还内嵌了网页过滤功能，可以防止公司员工访问不良网站，提高公司工作效率。

## 产品主要特性和优点

### 侠络客邮件安全产品的功能特点

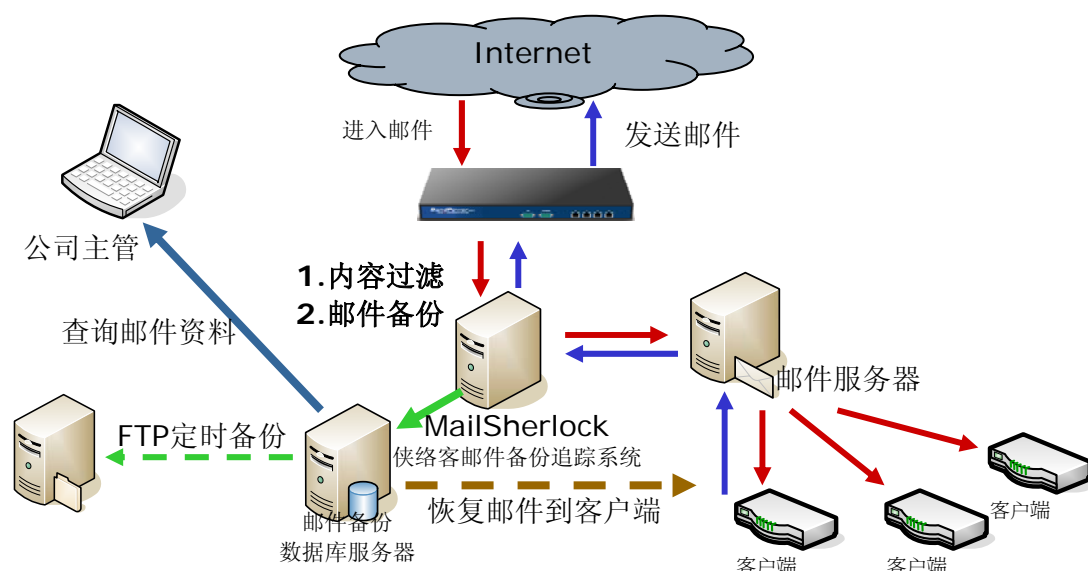
1. 通过 SMTP 转发方式，让进出邮件服务器的邮件，转移到侠络客邮件安全服务器上做查毒，内容过滤，防垃圾邮件检测，邮件备份的操作流程之后再发送。让进出邮件无一遗漏的保存到数据库中。
2. 高效的网关防毒模式 (VirusSherlock)，可以针对 HTTP/FTP/SMTP/POP3 的端口进行进出文件的完整杀毒，避免病毒对内部感染，而且一旦发现病毒攻击，可以立刻对来源 IP 进行封锁，保证内部安全
3. 个性化反垃圾邮件设定 (SpamSherlock)，每个员工可以根据自己的实际情况设定垃圾邮件过滤规则，从而降低网管人员的工作压力，也充分体现个性化的需求。
4. 利用层级管理模式，有效控制管理者查看的内容范围，可以对自己管辖部门以及子部门进行管理，由于层级的限制，避免越级或跨部门查看资料。
5. 细致的权限管理，建立群组的管理，方便分配管理者的管理权限，不用每次都要一一选，又可以针对个别管理者进行管理权限的详细设置工作，做到共性和个性的完美结合。
6. 快速的导入机制，利用 EXECL 软件编辑的 CVS 文件，把员工，部门信息可以在最快速的情况下，导入到系统中，为产品的导入工作降低了信息输入的工作强度。同时，也可以和微软的 AD (Active Directory) 建立帐户同步。
7. 提供多条件的邮件查询方法，做到全方位的邮件查询模式。为管理者快速查阅所需邮件提供有力帮助。
8. 丰富的统计报表模式，提供多种时间段的统计方式，可以根据进出流量、用户、部门等不同条件显示数据。而且图形化的显示方式让管理者一目了然。
9. 强力的过滤模式，提供邮件各种条件的过滤方式，支持隔离、删除和延后发送的处理机制。为管理人员对疑问邮件能够快速作出处理操作。
10. 有效的反垃圾邮件机制，利用多种反垃圾邮件手段，检测来往邮件的真实性，避免垃圾邮件的侵扰。
11. 完备的查毒机制，利用欧洲第一杀毒品牌 Sophos 杀毒引擎，快速过滤病毒邮件，并对病毒邮件做隔离，删除操作。并且对无法确定的疑问邮件提供隔离、删除、放行的选择。

12. 强大的备份功能，支持多种备份方式，包括立即备份和定时备份。支持磁带机和远程 FTP 备份模式。让你的备份工作，一次设定，自动备份。
13. 自动监控管理，对磁盘空间、运行程序进行实时监控，一旦出现问题或者磁盘空间超越临界点，立刻通过邮件通知系统管理员，确保系统稳定运行。
14. 定时自动更新，MailSherlock 可以设定自动更新机制，更新应用程序和病毒码，确保系统保持最新版本，降低安全风险。

# 实际应用的常用网络架构

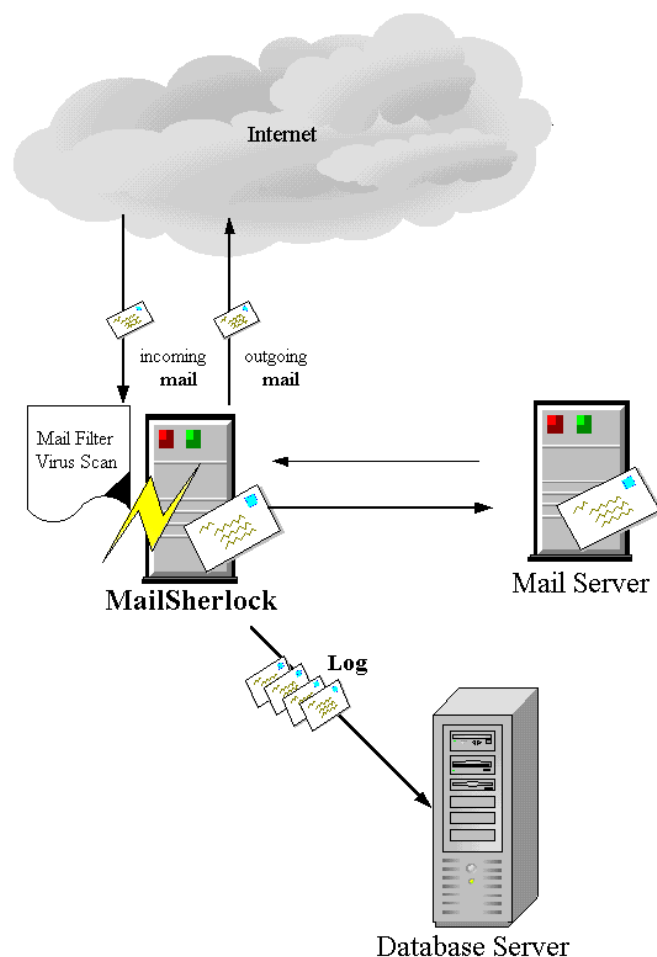
## 1. 基本架构

这是 MailSherlock 比较常用的设计架构，比较适合小型企业或者日常邮件量不多的用户。以网络架构而言，它相当于在邮件服务器之前建立了一个网关型的设备来保护邮件服务器的安全，外部进出的邮件会先经过 MailSherlock 进行反垃圾邮件监测、扫毒、过滤和备份操作完成之后，确认邮件安全后，才将信件递送到邮件服务器上，客户通过邮件服务器接收邮件。



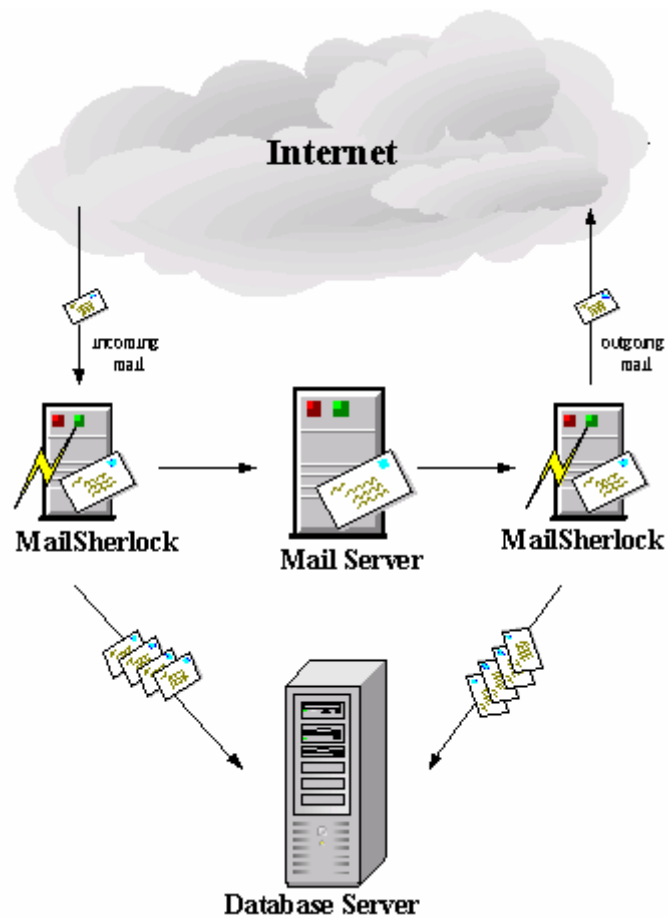
## 2. 数据库独立架构

这个架构主要针对有一定规模的企业、员工人数及邮件寄发量相对频繁，或者企业的在为了确保更好的扩展性，可特别针对保存邮件资料的数据库做弹性的规划，因为数据库的频繁读写，通常需要较大的系统资源，为增强系统运作效能，独立建立一台数据库服务器，专职于 **MailSherlock** 邮件记录，减轻 **MailSherlock** 的系统负载，而 **Mailsherlock** 前端仅负责邮件检查及病毒过滤、隔离的工作。做到分工合作，而且也方便了数据容量的扩展，同时确保在 **MailSherlock** 服务器出现意外故障的时候，数据不会丢失。**MailSherlock** 支持 HA 模式，可以通过 LVS(Linux 虚拟服务器)配置双机互备模式，确保 **MailSherlock** 的稳定运行。



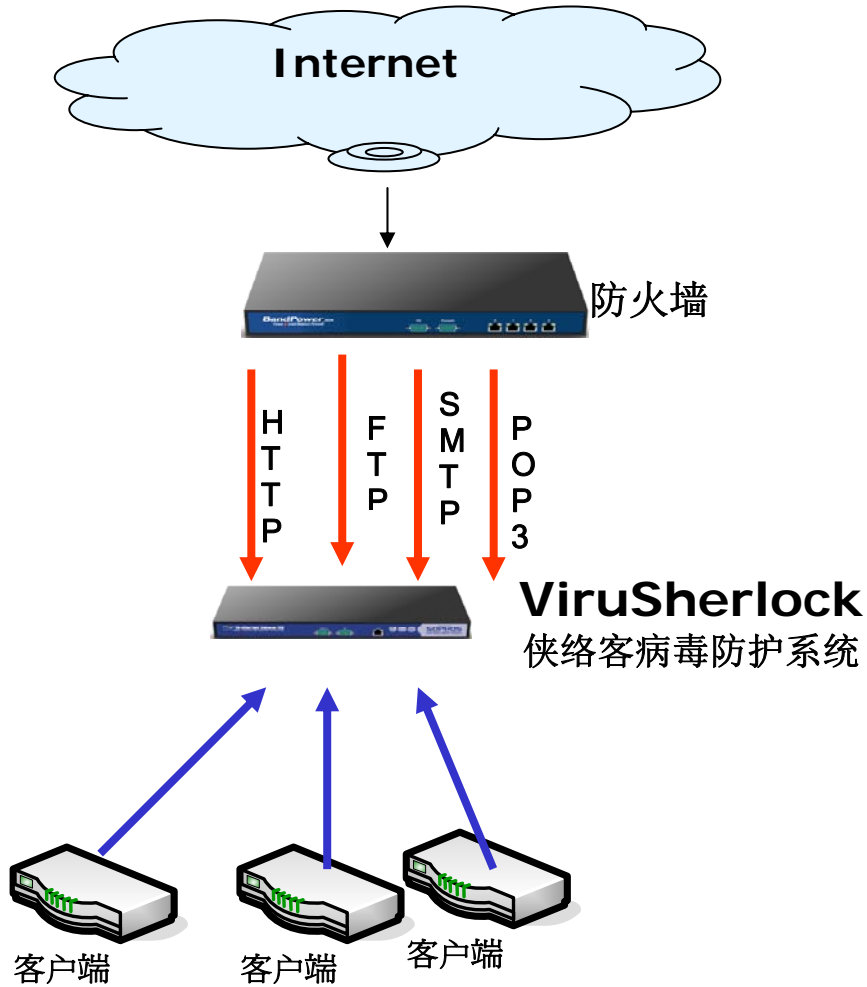
### 3. 进出分离架构

这种架构主要针对大企业，邮件账号在上千或者日邮件流量在 1GB 以上来设计的。规划两台 **MailSherlock** 分别负责进(incoming)、出(outgoing)邮件的过滤、隔离，可分散系统负载。另规划一台数据库服务器专职 **MailSherlock** 记录下来的邮件，使邮件数据统一储存、统一管理，并减轻两台 **MailSherlock** 服务器的系统负载。这样，邮件数据及公司全体人员账号资料仍能统一建立于数据库服务器，作为账号查询、邮件查询、统计报表、排行统计等功能运作的数据来源。对于需求量更大的企业，还可以设置 HA 模式，利用 LVS(Linux 虚拟服务器)来建立备份，分流的机制，确保系统的稳定运行。



## 网桥模式

网桥模式主要是针对需要防范网络病毒攻击的企业和部门所提供的专业产品，它通过安装在防火墙和内部交换机之间，对于所有进出的 HTTP/FTP/POP3/SMTP 的数据包进行病毒过滤，一旦发现病毒自动邮件报警给网管人员。比较适合与中小型企业和特定部门采用。



# 案例说明

## 1. 邮件备份解决方案

### 背景

某芯片研发公司，对于公司的技术资料的安全要求很高，网络的安全规划非常严密，公司内的人员除了邮件可以和外部连接之外，其它网络访问均被阻挡。由于邮件是和客户，供应商以及员工之间的信息交流平台。无法对他们做过于严密的限制，但同时存在安全的隐患。

### 需求

1. 邮件服务器使用Notes 系统，必须能支持该邮件系统收发信件。
2. 邮件处理能力必须能每分钟承载500 封以上邮件。
3. 由于使用的帐户高达2000 人，对于帐户的管理需要能够同步操作。
4. 此系统必须有效过滤敏感信件。
5. 管理人员可以管理自己权利范围以内的邮件信息，而不是网管人员。
6. 能够保障系统的稳定性，以及出现意外情况，可以快速恢复。

### 解决方案

网络设计方案如图所示：

1. 架设两台**MailSherlock** 服务器系统，以冗余的方式做互备，当其中一台出现错误时，另外一台立刻取代作为备援机。
2. 规划NAS 作为独立的数据库服务器，用于存放邮件信息，即使两台**MailSherlock** 系统都发生故障，邮件信息不会丢失。
3. MailSherlock支持LDAP，可以和邮件服务器的帐户做到同步设定。
4. 邮件拦截系统用于转发的邮件服务器 通常使用一般的Sendmail，每分钟的送信速度为100 封，本系统提供的Sendmail 经由最佳化调整，每分钟可达600 封邮件，可以负担庞大的信件量。

### 效益

1. 所有进出邮件均完整备份到数据库中，有效的过滤规则可以控制邮件进出，保障邮件安全。
2. 详细的权限设置，让每个登录的帐户只能够访问到自己管理的部门信息，而不是全部，包括网管人员。
3. 邮件传递无任何延迟，不影响日常运作。
4. 两台**MailSherlock** 做备份，系统安全有保障，即使硬件出错也能确保正常运作。
5. 邮件重导机制，在员工电脑出现故障后，可以通过MailSherlock将邮件恢复到员工信箱中。
6. 支持多种备份机制，可以利用磁带机，FTP等等方式备份邮件。确保邮件长期保存。