

KILL 过滤网关
(KILL Shield Gateway)

使用手册

北京冠群金辰软件有限公司

目录

第一章 KILL Shield Gateway 简介	1
关于病毒	1
什么是病毒.....	1
病毒种类.....	1
病毒感染的影响.....	2
防止病毒入侵的建议.....	3
电子邮件病毒与 KILL Shield Gateway	4
KILL Shield Gateway 简介	4
KILL Shield Gateway 是如何工作的.....	5
KILL Shield Gateway 的功能模块	8
KILL Shield Gateway 特点	8
冠群金辰企业级防病毒解决方案	11
欲知详情	12
第二章 KILL Shield Gateway 的安装	13
KILL Shield Gateway 的接入方式	13
KILL Shield Gateway 的外观	14
背部面板图.....	14
前部面板图.....	14
产品型号说明	14
系统说明	15
KILL Shield Gateway 安装前的准备工作	15
安全建议	15
安装场所必备条件	16
检查产品及附件.....	16
KILL Shield Gateway 的安装	16
KILL Shield Gateway 机架式安装	16
连接电源	17
连接以太网 10BASE-T 接口	17
下一步是什么？	18
第三章 KILL Shield Gateway 的配置与使用	19
面板的使用	19
连接/切断电源—Power 键	19
系统重新启动—Reset 键	19
时钟调节—Select 和 Adjust 按钮	19
系统信息显示与报警—发光二极管和液晶显示屏	19
KILL Shield Gateway 的启动与中止	21

KILL Shield Gateway 的配置管理界面	21
“基本系统” 页面	22
“用户管理” 页面	26
“过滤引擎” 配置页面	28
“邮件系统” 页面	32
“邮件域” 页面	33
“邮件传递” 页面	35
“邮件过滤” 配置页面	37
“邮件报表” 页面	39
“退出” 页面	42
KILL Shield Gateway 的帮助文档	43
第四章 KILL Shield Gateway 使用举例	43
用户网络环境概述	43
操作步骤	44
常见问题解答	47

版权声明

北京冠群金辰软件有限公司©2002-10-10

版权所有，保留一切权利。

北京冠群金辰软件有限公司拥有完全的著作权，未经本公司书面授权，任何个人或单位不得以任何形式复制、传播、提取、公开展示、出售本书的部分或者全部，否则一切后果违者自负。

KILL™为北京冠群金辰软件有限公司的注册商标，不得仿冒。

北京冠群金辰软件有限公司

2002-10-10

第一章 KILL Shield Gateway 简介

KILL Shield Gateway 是冠群金辰公司针对当前越来越猖狂的电子邮件病毒研发的电子邮件网关系统，该系统克服了目前众多杀毒厂家的反邮件病毒产品过于依赖邮件系统的缺点，根据邮件系统使用的协议而不是具体的邮件平台进行病毒查杀工作，接入简单，易于配置。

KILL Shield Gateway 采用独立的硬件平台，工作效率大大高于在邮件系统上安装反病毒软件的方式，而且采用冠群金辰备受赞誉的反病毒引擎，该扫描引擎经 ICSA（国际计算机安全协会）认证可“100%查杀流行病毒”，并获得全球 18 家重要测评机构的认证，使用安全可靠，是 KILL Shield Gateway 强大反病毒功能的基础。

KILL Shield Gateway 通过 Web 页面进行系统配置，管理界面友好，使用简便，易于配置，而且一旦配置完成，可自动完成病毒查杀、特征码下载、日志记录、报表生成等工作，大大减轻了网络安全管理员的负担，是一款技术极为先进的网关过滤产品。

关于病毒

什么是病毒

对任何计算机用户来说，计算机病毒都是威胁系统安全的主要因素之一。计算机病毒是一种计算机程序，就象生物学中的病毒，能够破坏计算机系统里的信息。它能够自行复制，并附着在其它文件上（通常是可执行程序）。如果将病毒进行隔离（不可执行，比如在一个压缩文件中）便不会产生危险，但一旦被打开，病毒便会产生破坏作用。

病毒文件具备以下特征：

- 可以自行复制
- 依附在其它可执行文件上

计算机病毒有多种类型，例如文件病毒、宏病毒、蠕虫及特洛伊感染等类型。

病毒种类

按照传播和感染方式的不同，病毒可分为多种类型，表 1-1 列出了常见病毒类型及其破坏作用：

病毒名称	描述
------	----

引导扇区病毒	这类病毒会将自己的特征码覆盖到磁盘的引导扇区（在引导扇区中有系统启动时要执行的代码），导致病毒总是被最先加载到内存中，这就意味着你每次开机时病毒就会运行。一旦病毒进入内存就会导致启动磁盘无法使用，并可能将病毒传播到其它磁盘中。
主引导区病毒	这类病毒改写磁盘中的主引导扇区（分区表）。它们很难被检测到，因为大多数磁盘检测工具不能查看分区表。
宏病毒	这类病毒写入到特定计算机程序的宏语言中，比如文字处理软件或电子数据。宏病毒是感染文件而不是感染引导区或分区表，而且一旦被执行便常驻内存。当用户访问或使用被宏病毒感染文件时，宏病毒便会运行（比如按键或菜单的操作）。宏病毒存贮在文件中，通过文件传播，包括以电子邮件形式进行传播。
文件病毒	这类病毒会在运行一个受其感染的程序时传染其它程序。它们不会驻留在内存中，因此不会感染系统。非驻留内存病毒与常驻内存病毒一样附着在可执行文件上，通常会改变文件的属性、大小、时间以及日期等信息。
复合型病毒	这类病毒具有常驻内存病毒、文件病毒和引导区病毒等多种病毒的特征

表 1-1 常见病毒类型及其说明

其它的病毒类型还包括蠕虫，DDOS 等。蠕虫与病毒相似，它们都会自我复制。一旦蠕虫被执行，它会传染其它任何系统。DDOS 攻击不受怀疑的系统隐藏文件。在将来某个时候这些隐藏文件被激活时 DDOS 病毒便会对系统产生恶意的破坏。

病毒感染的影响

并非所有的病毒感染都危害你的计算机。一些只是令人讨厌，在屏幕上显示出奇怪的图案或信息。大多数病毒在没有运行时都是处于隐藏状态。计算机病毒对计算机有以下破坏作用：

- 中止计算机运行
- 删除、修改或隐藏你的文件
- 破坏硬盘上的数据
- 攻击并破坏文件分配表
- 攻击并破坏分区表
- 格式化硬盘
- 不断地自我复制

随着网络的高速发展，网络病毒也应运而生。与传统类型病毒相比，网络病毒在具体的表现形式、传播路径和破坏目标方面有所不同，它主要通过邮件、Internet、局域网等传播，而不是通过传统的介质传播，因而具有传播快，影响力大的特点，被越来越多地病毒制造者采用，逐步替代了传统病毒。在过去的一段时间中，Nimda(尼姆达)，CodeRed(红色代码)，HappyTime(欢乐时光)，Klez(求职信)等病毒都曾在全球范围大规模爆发过，病毒产生的大量网络流量造成网络的过度拥堵，许多用户因此无法提供正常网络服务，甚至造成网络瘫痪，造成难以估计的损失。

防止病毒入侵的建议

以下是帮助个人电脑远离病毒的一些建议：

- 从软盘上拷贝任何文件之前先进行病毒扫描。
- 在你成功地完成病毒扫描之后用备份工具（例如 ARCserveIT）备份你的计算机系统。这样，在某一文件感染了无法修复的病毒时，可用已有的备份文件进行恢复。
- 让你的计算机工作保持最新的病毒特征码。
- 通过设置访问权限来管理你的共享目录，让用户对该共享目录有合适的权限等级，例如只有只读权限而不是完全访问控制权限。
- 如果发现了可能有病毒的文件，而且你希望将这文件交给冠群金辰公司进行病毒分析的话，请用 AVB 文件扩展名对其重命名，并在向外发电子邮件或存入软盘之前对文件进行压缩处理。

对于企业级网络防病毒，则要建立起全面立体的防病毒体系，请参见本章的“冠群金辰企业级解决方案”一节。

电子邮件病毒与 KILL Shield Gateway

Internet 的普及与企业电子邮件的广泛使用，快速增加了企业竞争力与生产力，但同样也让计算机病毒找到更快速的传染媒介。附带有病毒文件的电子邮件，往往在短时间内一传十、十传百，造成多米诺骨牌效应式连锁感染，因此成为目前主要的病毒传播方式。

一项由国际计算机安全协会（ICSA, International Computer Security Association）所公布的「2000 年度病毒传播趋势报告」结果显示，电子邮件已跃升为计算机病毒最主要的传播媒介，感染率由 1998 年的 32%，1999 年的 56%，大幅成长至 2000 年的 87%，引人注目；传统经由磁盘、网络下载的病毒感染方式则急剧下降。（见表 1-2）

病毒来源	1996 年	1997 年	1998 年	1999 年	2000 年
磁盘	74%	88%	67%	39%	7%
E-mail	26%	26%	32%	56%	87%
Internet 下载	12%	18%	12%	13%	2%
其它	15%	20%	11%	13%	4%

表 1-2 1996 年~2000 年计算机病毒传播媒介比率 ICSA 统计报告

通过 email 大量散播的病毒类型包括“宏病毒”、“文件型病毒”、“VBS 病毒”及“JavaScript 蠕虫”等。这种病毒类型在 1998 年随着 Happy 99(Win32/Ska)病毒扩散而首次现身；1999 年 3 月伴随着梅莉莎病毒事件后日益流行；2000 年的 ILOVEYOU 病毒及 2002 年的求职信病毒更是肆虐全球。该类型病毒通常通过邮件客户端，发送大量的垃圾邮件，使邮件服务器不堪重负，进而影响网络正常运作。如何在邮件服务器上做最好的防护，成为各反病毒厂家的最重要的课题之一。

KILL Shield Gateway 简介

针对电子邮件已成为最常用的病毒传播方式这种状况，各反病毒厂家都在积极开发邮件服务器上的反病毒产品，在保证邮件系统安全的同时，也带来一些问题：

- 邮件服务器负担的增加-- 杀毒任务的引入，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支持查病毒引擎的工作，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。

- 开发成本高-- 邮件系统多种多样,如 Notes、Exchange、Sendmail、Qmail、Postfix 等都有相当的使用用户,同时邮件系统又是相当复杂的系统,如果要开发防病毒软件,不同类型的邮件服务器需要开发不同的防病毒软件,造成开发成本大大提高。
- 用户资源的重复建设-- 由于不同的邮件系统需要不同的防病毒软件,当邮件系统升级或改用另外一种邮件系统时,用户通常不得不重新购买相应的防病毒软件,造成用户资源的浪费。
- 邮件系统的稳定性降低-- 邮件服务器是企业网络的核心服务器,在核心服务器上频繁地安装和卸载软件显然是有相当风险的。

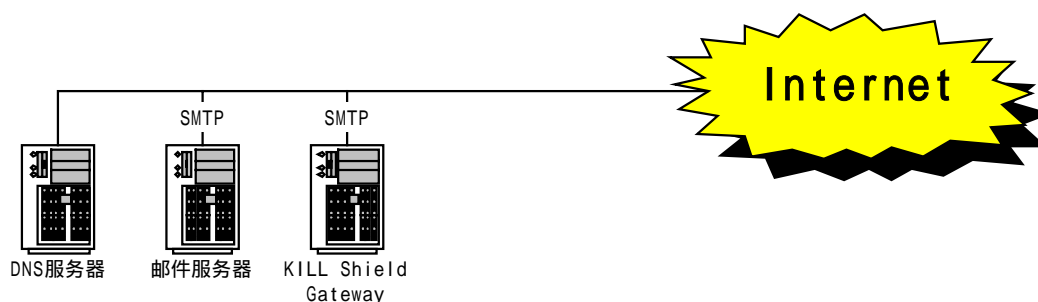
冠群金辰推出的与邮件系统类型无关的邮件防病毒产品--KILL Shield Gateway,解决了上述问题。它使用独立的硬件平台进行病毒的查杀工作,确保了原有邮件系统的稳定性,并在效率方面远远高于在邮件服务器上安装防病毒软件的方式。它针对 SMTP 协议进行邮件过滤,其应用只与是否使用 SMTP 协议有关,而与具体的邮件系统无关。使用 KILL Shield Gateway,一旦安装和配置完成,无需值守,无需手工操作,可实现自动升级,自动发现、清除病毒,自动报警,时时刻刻保护您的邮件系统。

除了正常的查杀病毒工作,KILL Shield Gateway 还可增加其它过滤引擎,进行功能扩展(如:敏感信息邮件过滤、垃圾邮件过滤等)。同时,用户还可以通过均衡和集群线性地扩大 KILL Shield Gateway 的处理能力。在对 SMTP 协议的支持上,当前 KILL Shield Gateway 支持标准的 SMTP 和 SMTP 的扩展协议---ESMTP。

KILL Shield Gateway 是如何工作的

KILL Shield 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值稍大的 MX 邮件服务器;同时邮件总是在同一优先级的 MX 邮件服务器都尝试失败后,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 KILL Shield Gateway 最高的优先级,KILL Shield Gateway 具有完整的 MTA 服务功能,这样所有的邮件将先发到 KILL Shield Gateway,进行查杀毒处理,再由 KILL Shield Gateway 通过 SMTP 协议传给 MX 邮件服务器。KILL Shield

Gateway 典型的接入方式如下图 1-1 所示：



注：邮件服务器的优先级在 DNS 服务器中设置。

图 1-1 KILL Shield Gateway 典型的接入方式

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 KILL Shield Gateway 就可以了。

显然，这种方式在满足防范邮件病毒的同时，规避了在邮件服务器上安装防病毒软件带来的问题，它只针对 SMTP 协议进行邮件过滤，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防病毒软件而言，具有更高的查杀毒效率。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 KILL Shield Gateway，保护了用户的已有投资。

KILL Shield Gateway 在接收到邮件后的大致工作流程如图 1-2 所示：

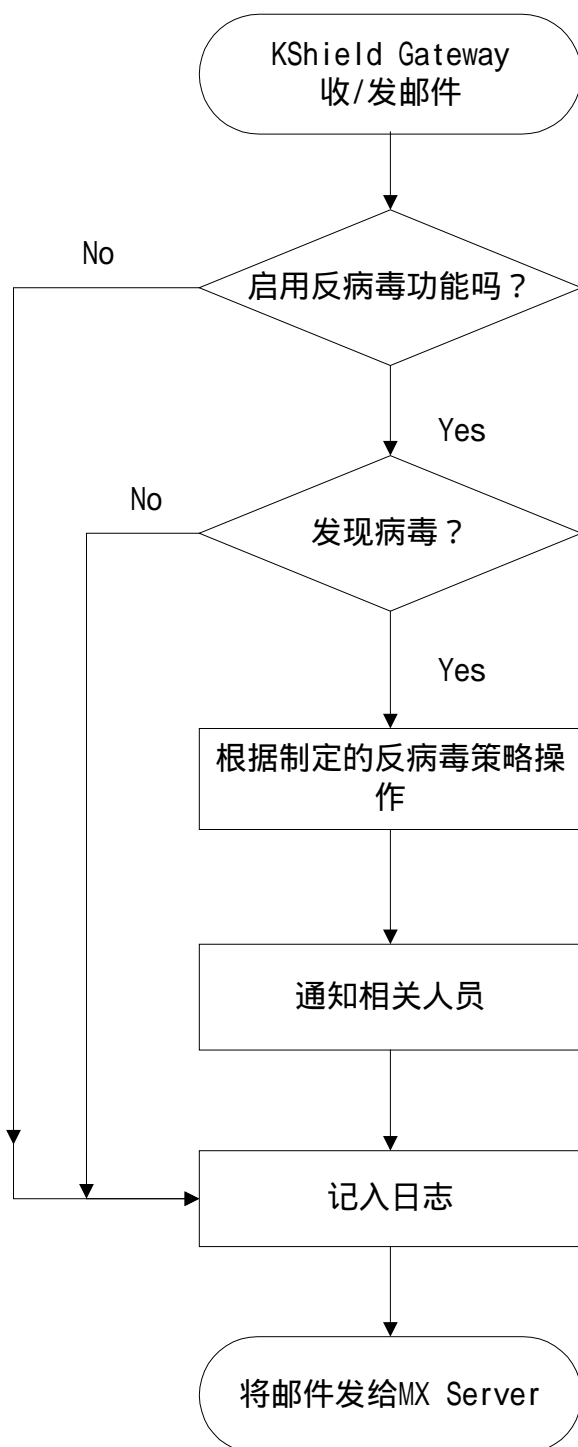


图 1-2 KILL Shield Gateway 邮件病毒处理流程

KILL Shield Gateway 邮件网关系统采用有规则、多形、可分析等病毒扫描措施来检测已知病毒,其病毒扫描引擎经 ICISA(国际计算机安全协会)认证,可“100%查杀流行病毒”,通过对邮件系统提供不间断的病毒防护,保证企业邮件系统的安全和稳定。

KILL Shield Gateway 的功能模块

KILL Shield Gateway 功能的实现主要依靠以下功能模块：

- **系统配置** 采用 B/S 结构，使用浏览器进行 KILL Shield Gateway 系统本身的配置，还可对邮件系统，过滤引擎，报表等进行配置，用户无需输入命令行，操作简单，界面友好。配置工作可在本地或远程进行。
- **扫描系统** 对于已知病毒采用基于规则的扫描引擎进行扫描，实时检查往来邮件中是否含有病毒。
- **邮件处理** 可以决定如何处理受到病毒感染的文件，包括修复、删除等，病毒处理方式灵活多样。
- **通知** 对发现带有病毒的邮件，可根据设置通知给发件人、收件人和邮件系统管理员，以便采取相应的安全措施。
- **报告** 完善的报告机制记录了所有的病毒扫描活动，为病毒的跟踪和分析提供了可能。
- **特征码更新** 特征码更新操作可通过冠群金辰公司的网站定期进行。该过程可根据事先设好的时间自动进行，无需用户干预。
- **SMTP 认证** 如果原邮件服务器要求对通过该邮件服务器转发邮件的用户身份进行认证，即 SMTP 认证，在引入了 KILL Shield Gateway 之后，该认证过程将由 KIShield Gateway 来进行。它会将认证过程的数据流重新定向给认证服务器，并根据认证的结果来决定是否接收用户的发信请求。即使原邮件服务器不支持 SMTP 认证，仍可以使用 KILL Shield Gateway 的 SMTP 认证扩展模块，将 SMTP 认证协议转变为对 POP3 用户或对 Windows 域用户的认证协议，进行发信认证。认证的过程完全遵循 ESMTP 的认证协议标准。
- **WatchDog** KILL Shield Gateway 设计有软件 WatchDog，当 KILL Shield Gateway 的活动进程在意外情况下僵死时，WatchDog 会按照一定的策略自动去重新启动该进程。系统具有一定的自维护能力。

KILL Shield Gateway 特点

➤ 友好的系统管理界面

对邮件系统的管理采用 B/S 方式，用户可使用浏览器本地或远程修改 KILL Shield Gateway 系统本身配置及各项反病毒策略的配置，用户界面友好，操作简单。

➤ 卓越的病毒查杀能力

KILL Shield Gateway 的反病毒引擎获得了 ICISA（国际计算机安全协会）实验室的查杀病毒认证，能够 100% 地检测出目前“流行病毒名单”上的病毒，确保用户关

键数据和服务的安全。

➤ 更高的查杀毒效率

KILL Shield Gateway 使用独立的硬件平台进行邮件病毒的查杀工作，无需占用邮件服务器的系统资源，一方面确保了原邮件服务器的稳定性，另一方面大大提高了查杀毒效率，其效率远远高于在邮件服务器上安装防病毒软件的方式。

➤ 接入方式简单易行

KILL Shield Gateway 的接入方式非常简单，通常无须修改邮件服务器的任何配置，即可开始进行邮件的病毒查杀工作。此外，由于其工作与使用的邮件服务器的具体类型无关，即使用户更换了新的邮件服务器，也无需更换 KILL Shield Gateway，从而保护用户的已有投资。

➤ 实时查杀病毒及报警

KILL Shield Gateway 实时查杀邮件服务器接收到的新邮件中所含有的计算机病毒，阻止病毒通过邮件进入到用户计算机，并可根据邮件管理员的设置报警，将病毒信息通知给发件人、收件人或管理员，以便采取适当措施，保证邮件系统的安全。

➤ 灵活的病毒处理方法

对检测出含病毒的邮件可根据用户的设置进行清除病毒、删除附件、丢弃邮件等操作，如果操作设为清除病毒，则还可选择一旦清除病毒失败后 KILL Shield Gateway 应采取的操作，确保邮件安全。

➤ 自动更新病毒特征码

任何的病毒扫描引擎皆须配合最新的病毒特征码来维持最有效的扫描效能，所以定期更新病毒特征码对于保持系统的安全非常重要。KILL Shield Gateway 可通过冠群金辰网站，根据管理员定义的更新频率与策略，自动更新病毒特征码，确保始终使用最新的病毒特征码对邮件进行病毒检查，使邮件免受各种新病毒的侵害。

➤ 完整的病毒事件记录

KILL Shield Gateway 提供一份详尽且完整的病毒事件记录报告，包括：

- 邮件序号
- 发生日期

- 发件人
- 收件人
- 病毒名称
- 采取的行动(治愈，删除等)

KILL Shield Gateway 还提供根据这些数据生成图形化统计报表的功能。

➤ 丰富的报表

KILL Shield Gateway 面向网络管理人员提供丰富的图形化报表，包括：

- 病毒邮件比例报表
- 内部带毒邮件账户报表
- 外部带毒邮件账户报表
- 病毒邮件时段分布报表
- 病毒邮件趋势报表等。

这些报表形象直观，便于管理员了解邮件系统的使用状况，制定相应的安全策略。

➤ 完善的自保护机制

KILL Shield Gateway 设计有软件 WatchDog，具备自维护能力。当 KILL Shield Gateway 的活动进程在意外情况下僵死时，WatchDog 会按照一定的策略自动重新启动该进程，确保系统本身的稳定性。

➤ 自适应

当发生邮件风暴的时候，同时处理大量的并发邮件会达到 KILL Shield Gateway 的并发处理极限。KILL Shield Gateway 会检测系统资源的消耗情况，当达到处理极限后，KILL Shield Gateway 会将新来的邮件先放入等待过滤队列而不马上进行处理，当系统资源有空闲后，再激活等待过滤队列中的邮件进行处理。

➤ 管理多个域

在大型企业、ISP 和 ASP 的邮件系统实现中，常常使用一个或多个 MTA 对多个域提供服务。KILL Shield Gateway 的多域管理模块完全实现了 MTA 的这一技术，可以同时支持对多个域的邮件病毒过滤，在使用集群模块的情况下，可以使用多台 KILL Shield Gateway 保护多个域的多个 MTA。

➤ 支持 SMTP 认证

为防止垃圾邮件泛滥等滥用邮件系统的行为,许多邮件系统在接受用户的发信请求前,要求对用户的身份作认证,即 SMTP 认证。如果原有邮件服务器进行 SMTP 认证,在引入了 KILL Shield Gateway 之后,该认证过程将由 KILL Shield Gateway 来进行。它将认证过程的数据流重定向给原邮件服务器,并根据认证的结果来决定是否接收用户的发信请求。

如果用户的 RELAY 邮件服务器不支持 SMTP 认证,可以使用 KILL Shield Gateway 的 SMTP 认证扩展模块,将 SMTP 认证协议转变为对 POP3 用户或对 Windows 域用户的认证协议,进行发信认证。

➤ 过滤引擎扩充

KILL Shield Gateway 的过滤引擎是可以扩充的,除了病毒过滤引擎,还可以加入色情图片过滤引擎,及倾向性言论过滤引擎和垃圾邮件过滤引擎。KILL Shield Gateway 的过滤器和过滤引擎可以位于不同的主机上,以减少对过滤器主机资源的消耗,满足超大邮件系统过滤的要求。

➤ 容错、均衡与集群

KILL Shield Gateway 具有很强的容错能力,其容错处理主要体现在两方面,一是和原有邮件服务器的容错,二是使用多台 KILL Shield Gateway 时的容错处理,确保用户可始终正常收发邮件。此外,当用户邮件系统负载过重时,可采用多个 KILL Shield Gateway 实现自动负载均衡,并通过集群模块,使各 KILL Shield Gateway 有相同的策略配置,并可以生成统一的邮件病毒情况报表。

冠群金辰企业级防病毒解决方案

面临新型网络病毒的种种危害,着眼于单机防毒的传统防毒策略经常无法奏效。企业若要建构完整的网络安全环境,不应让内部个人计算机端防毒软件成为唯一的安全防线,而必须兼顾网络上每个节点的防毒工作,从单机个人计算机、局域网络服务器、电子邮件服务器至 Internet 网关,将防毒软件集中控管,以建立完整的网络防毒架构,才能确保网络安全,同时降低企业管理成本。

冠群金辰作为著名的防毒软件厂商,长期以来专注于防毒技术研发,其产品多次获得国内外国际权威机构的高度肯定。冠群金辰公司 KILL 系列防病毒产品为企业网络及个人计算机提供了强大的防病毒解决方案。它可以有效地保护 Windows NT/2000/XP、Windows 95/98/Me、Windows 3.x、DOS 和 Macintosh 等系统,还具有 Novell Netware、Linux 和 Unix 等系统的防病毒版本。在邮件方面,不仅有针对 Lotus Notes、Microsoft Exchange 等邮件服务

器的防病毒产品，更开发了功能强大的邮件网关产品—KILL Shield Gateway，从而形成了全面立体式防病毒体系，在各个环节上都可保证用户企业网络的安全，为企业用户提供网络防病毒系统的全面解决方案。

欲知详情

浏览了本使用指南后，您可以参见许多其他资源以获得详细信息。KILL Shield Gateway 还有很多有价值的指导性文档，如技术白皮书等，针对“邮件系统安全”的实现原理和工作方式做了全面详尽的解释。此外，联机帮助针对您实际使用中可能遇到的问题提供了详细信息和问题解答。

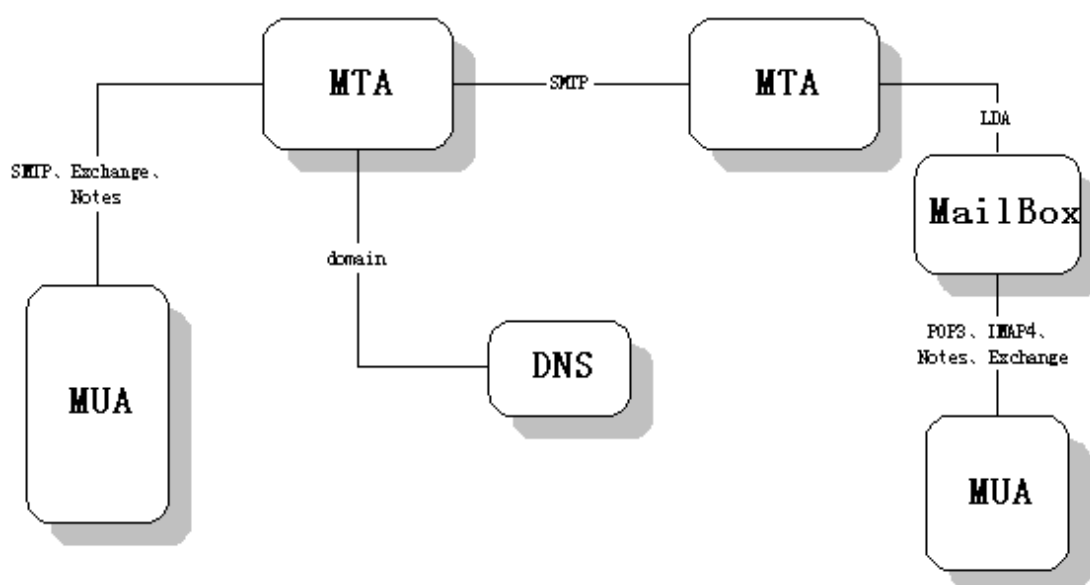
一旦发现病毒感染，可以在冠群金辰公司网站上获取有关病毒、蠕虫、特洛伊木马的更多信息。我们的 web 站点：www.kill.com.cn 中也含有对产品的简单介绍。

如果您需要技术支持，请拨打热线：(010) 65612426, (010) 65612408。传真：(010) 65612410。

第二章 KILL Shield Gateway 的安装

KILL Shield Gateway 的接入方式

首先我们了解一下通常电子邮件的传输过程,即邮件客户端 MUA 使用 SMTP、Exchange 或 Notes 传输协议将邮件发给 MTA (类似现实生活中的邮局), MTA 解析邮件头(相当于现实生活中的信封)得到目标地址,查找 DNS 服务器(现实生活中的邮政编码地址对照表)搞清楚可以接受该邮件的另一个 MTA,通过 SMTP 协议将 Email 传给这个 MTA,收信人的 MUA 再通过 POP3 或 IMAP4 协议读取邮件。如下图 2-1 所示:



其中,我们称发邮件的 MTA 为 RELAY 邮件服务器,收邮件 MTA 为 MX 邮件服务器。

图 2-1 电子邮件的传输过程

了解了这一传输过程,我们就比较清楚 KILL Shield Gateway 的工作原理和工作方式了。KILL Shield Gateway 针对 SMTP 协议的邮件进行病毒过滤,其典型安装方式参见第一章“KILL Shield Gateway 是如何工作的”一节介绍,接入方式极其简单,只需:

- 与原有的 MX 服务器处于并联关系
- 修改 DNS 配置,赋予 KILL Shield Gateway 最高的优先级
- 赋予 KILL Shield Gateway 一个公用 IP

下面就介绍 KILL Shield Gateway 的具体安装过程。

KILL Shield Gateway 的外观

背部面板图



图 2-2 KILL Shield Gateway 的背部面板

前部面板图



图 2-3 KILL Shield Gateway 的前部面板

产品型号说明

本说明文档介绍邮件过滤网关的两个产品型号，即 406 型号和 408 型号。其中 406 为针

对单域的邮件过滤，408 为针对多域的邮件过滤产品，不同的域可采用不同的过滤策略，因此二者界面也略有不同，但实现的过滤功能相同。和它们相对应的，还有 600 系列和 800 系列产品，分别为 406 和 408 型号的硬件高端产品系列，以满足用户更大数据量和更快处理速度的需求。

系统说明

对 KILL Shield Gateway 的基本配置，外形尺寸和工作环境等项目的描述如表 2-1 所示。

项目	描述
接口	1 个以太网口 1 个 VGA 口 1 个 USB 接口
处理器	Intel PIII 866
显示屏	1 个 A78A Panel LCD/A106 Alarm board
外形尺寸	440×431×44(W×D×H)(mm)
操作温度	0~40 摄氏度
相对湿度	5~95% (RH)

表 2-1 KILL Shield Gateway 的基本配置

KILL Shield Gateway 安装前的准备工作



注意：

为避免出现意外情况造成人身损害或设备损坏，请在安装 KILL Shield Gateway 前仔细阅读本节内容。

安全建议

在 KILL Shield Gateway 的安装和使用过程中，特提出如下的安全建议：

- 请不要将 KILL Shield Gateway 放置在有水的地方，也不要让液体进入机箱内。
- 请将 KILL Shield Gateway 放置在远离热源的地方。
- 请不要带电插拔电缆。
- 请注意用电安全。
- 建议用户使用 UPS 不间断电源。

安装场所必备条件

KILL Shield Gateway 安装场所应具备如下的条件：

- 请将 KILL Shield Gateway 放置在平坦、干净的固定平台或固定在机架上，KILL Shield Gateway 跌落可能造成严重损坏。
- 须将 KILL Shield Gateway 放置在清洁和通风的环境中。

检查产品及附件

在确认安装环境符合要求后，您可以打开包装箱了。但在正式安装之前，您还需仔细检查包装箱内的产品及附件是否齐全。

对于 KILL Shield Gateway，应包含内容如表 2-2 中所示。

项目	名称	数量	说明
1	KILL Shield Gateway 主机	1 台	产品主机
2	技术资料	1 套	用户手册
3	AC 电源线	1 根	
4	L 型支架和螺丝钉	1 袋（含 1 对支架）	

表 2-2 KILL Shield Gateway 包装箱内组件

建议您对照装箱单及订货合同核对您的货物。如有疑问或差错，请与销售商联系。

KILL Shield Gateway 的安装

KILL Shield Gateway 机架式安装

KILL Shield Gateway 满足 EIA 标准尺寸，可以像其他设备一样安装在 19 英寸的机架上，或放置在平坦的机柜架上。

如果要安装在机架上，安装时，将 KILL Shield Gateway 前面板向前放在支架上。为安全起见，扣上所提供的螺丝钉。如图 2-4 所示。

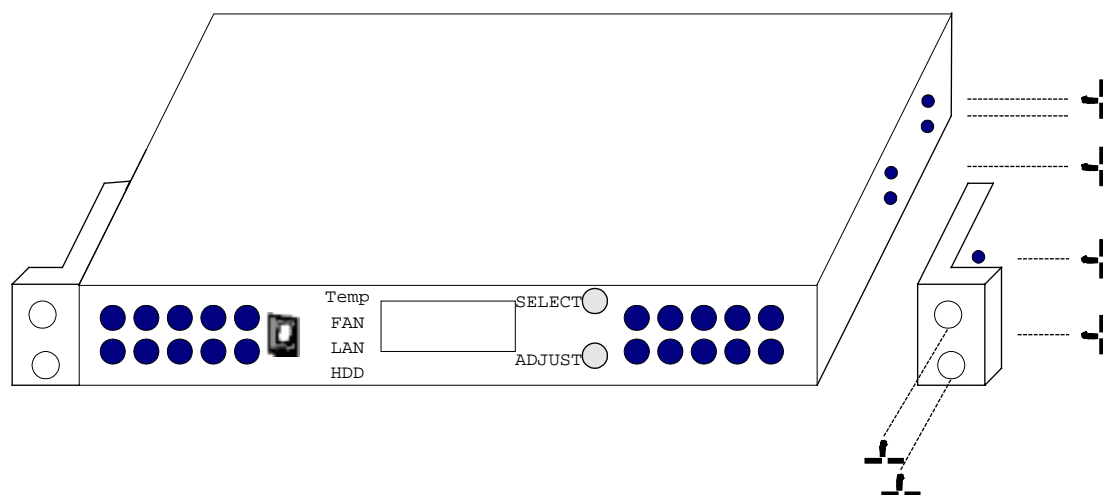


图 2-4 KILL Shield Gateway 的机架式安装

连接电源

请遵循以下步骤连接并接通电源：

第一步：请把电源线的输出端插头连接到 KILL Shield Gateway 背部面板的电源插座，将输入插头插入到 220V 电源插座。

第二步：请触击 KILL Shield Gateway 电源开关，启动系统。

第三步：检查前面板指示灯或显示屏是否变亮，如未亮请检查第一至第二步。

连接以太网 10BASE-T 接口

请遵循以下步骤连接以太网口：

第一步：请将以太网电缆的一端插入 KILL Shield Gateway 的 10 BASE-T 接口。

第二步：请将以太网电缆的另一端插入集线器(HUB)的 10BASE-T 接口。

第三步：请检查 KILL Shield Gateway 后面板的 10BASE-T 指示灯亮。

 **注意：**如反复重复上述步骤后电源始终无法接通，请与销售商联系。

 **注意：**请不要带电插拔电缆。

 **注意：**请不要擅自打开 KILL Shield Gateway 机箱盖，产品如出现故障请与销售商联系。

下一步是什么？

至此，我们已完成了 KILL Shield Gateway 的安装工作，下面就要带着您开始进行相应的配置，以满足您的网络的实际情况，使 KILL Shield Gateway 开始工作，实施对电子邮件系统的安全保护。

第三章 KILL Shield Gateway 的配置与使用

面板的使用

这里主要介绍前面板上各按钮的含义及使用方法。各按钮所在位置，请参见第二章“KILL Shield Gateway 外观”一节中的图示。下面按各按钮的功能进行介绍。

连接/切断电源—Power 键

使用电源开关 (Power) 连接/切断电源，该开关为轻触式电源开关，用户只需轻击该开关即可接通/切断电源。

系统重启动—Reset 键

当因为某种意外情况，造成系统宕机时，可使用该键重新启动系统。为避免用户误操作，将该键凹在面板内部，须重启系统时，使用尖状物伸入到孔中击一下该键即可。

时钟调节—Select 和 Adjust 按钮

这两个按钮协作，用于调整液晶显示屏 (LCD) 上的时钟。在 LCD 模块上集成了一个时钟，提供年、月、日、时、分、秒的信息。它还配备了可持续使用三年的电池。用户可通过前面板的两个按钮手动调整时钟。

第一步：按住上面的按钮 (Select) 3 秒钟以上，直到 LCD 显示屏上有一个光标在闪烁。

第二步：按下面的按钮 (Adjust)，调节时间。

第三步：再次按住上面的按钮，将闪烁的光标移动到下一位置。

第四步：重复步骤二和三。

第五步：设好时钟后，再次按住 Select 按钮 3 秒钟以上，离开编辑模式，直到光标消失，时钟开始运行。

系统信息显示与报警—发光二极管和液晶显示屏

KILL Shield Gateway 采用液晶显示屏显示系统信息，当监测到机箱内部的不正常情况时，一方面在液晶显示屏显示相关报警信息，另一方面前面板上的相关发光二极管闪烁，以示警告。下面详细介绍。

显示系统信息

为便于用户时刻了解系统内部工作状态，KILL Shield Gateway 采用液晶显示屏将信息显示出来。正常工作时，该屏循环显示两页信息：

第一页包括公司名称，产品型号，日期与时间。

第二页包括风扇转速（RPM），机箱温度，日期与时间。

报警

对机箱内温度的报警

机箱内的温度对系统的稳定运行起着重要的保证作用，为此 KILL Shield Gateway 时刻监视机箱内温度，机箱内有两个温度探头，当任一个的温度超过 70 摄氏度时，系统都会峰鸣报警，前面板的 **Temp** 指示灯闪烁，同时在液晶显示屏上显示报警信息，如图：



表示：第一个温度探头周围的温度已超过 70 摄氏度，必须采取相关措施，降低机箱内温度。

对风扇运行情况的报警

在 KILL Shield Gateway 机箱内，为保证机箱内温度符合要求，采用了四个风扇，本系统时刻监视这四个风扇的运行情况，一旦发现任一个风扇转速低于 1000 转/分时，系统都会峰鸣报警，前面板的 **Fan** 指示灯闪烁，同时在液晶显示屏上显示报警信息，如图：



表示：第一个风扇的运转出现问题，须采取相关措施。

对系统运行状况的报警

为保证对邮件系统病毒的持续查杀工作，KILL Shield Gateway 包含 WatchDog 功能，启用该功能后，将定期向系统发送轮询消息，并等待系统回应。如果系统在 Watchdog 发送了 5 次轮询后都未能及时回应，则 Watchdog 认为系统已宕掉，启动其报警程序，如峰鸣，以及在液晶显示屏上显示报警信息，如图：

**Warning
System Holding**

促使管理员迅速采取措施，重新启动 KILL Shield Gateway，以确保邮件病毒的查杀工作正常进行。

KILL Shield Gateway 的启动与中止

缺省情况下，开机时 KILL Shield Gateway 自动运行，由于在 DNS 中已将它的优先级设为高于原邮件服务器的优先级，邮件首先到达 KILL Shield Gateway，它根据事先设好的策略实时进行电子邮件病毒查杀工作。要中止其运行，可在配置管理界面的“系统配置”页中，点击“关机”即可。请参见下一节“配置管理界面”中的具体内容。

KILL Shield Gateway 的配置管理界面

KILL Shield Gateway 在设计上尽可能做到对用户友好，并且强调表达的清晰度和数据访问的方便性。它采用 B/W 管理方式，用户可从任何一台和 KILL Shield Gateway 联网的机器上，在浏览器的地址栏中键入 *https://KILL Shield Gateway 的机器名或 IP 地址(初设为 172.16.88.88,用户可连接后修改IP)*，就可以登录到 KILL Shield Gateway 的配置管理界面。

首先出现的登录界面，如图 3-1 所示。

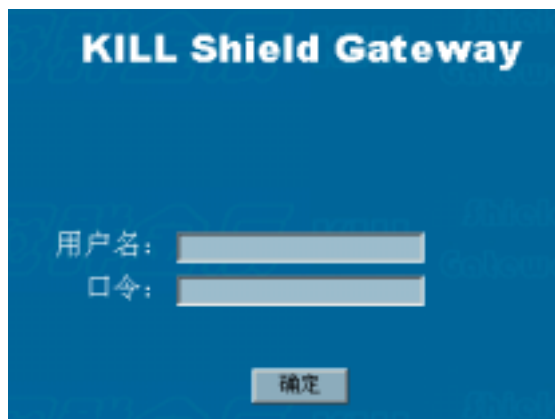


图 3-1 KILL Shield Gateway 的登录界面

必须是授权用户才可以浏览和修改 KILL Shield Gateway 的配置，如果是第一次登录，请在用户名栏中输入“admin”，口令为“killksg”。登录后请立即进入到“用户管理”页修改管理员口令，以确保管理的安全性。

配置管理界面根据功能分为多个页面，分别是：

- “基本系统”页面
- “用户管理”页面
- “过滤引擎”页面
- “邮件系统”页面
- “邮件域”页面（仅 408 型号有此管理页面）
- “邮件传递”页面
- “邮件过滤”页面
- “邮件报表”页面
- “退出”页面

下面详细介绍各页面的内容。

“基本系统”页面

登录到 KILL Shield Gateway 的管理界面后，首先显示的就是“基本系统”页面，在该页中可查看系统状态、产品信息，配置网络、设置域名解析、系统时间等，使 KILL Shield Gateway 本身的网络设置符合用户网络的实际情况。下面逐一介绍。

查看系统状态

在系统配置界面，点击“系统状态”可查看当前系统的运行情况和一些硬件信息。包括以下内容（见图 3-2）：



图 3-2 KILL Shield Gateway 的“系统状态”页面

运行状态：包括系统的主机名，已持续运行时间，平均负载情况等。其中平均负载参数很重要，它显示的是过去 1 分钟、5 分钟和 15 分钟的平均系统负载。可能的最小值为 0，最大值不限，但一般单处理器的平均系统负载不应超过 2，否则系统负载过重，会影响工作效率，这时 KILL Shield Gateway 将以红色显示该负载值，以示警告，管理员应检查原因，避免该情况发生。

网络状态：包括产品的网卡号、收到的流量、发出的流量、出错/丢失的流量等，根据用户网络，KILL Shield Gateway 可使用多块网卡，在网络状态中将显示每块网卡的相关数据。如果发现某网卡出现“出错/丢失”的流量，应立即检查网卡或网线是否工作正常，如有问题应及时更换，以免造成用户损失。

内存状态：包括物理内存使用情况，虚拟内存的使用情况等，这些参数对系统性能和运行速度有重要意义，应该使虚拟内存保持在 30% 的负载以下，才能保证系统的良好性能。

磁盘状态：包括系统区、数据区已用空间占各自总空间的百分比。该参数便于用户了解硬盘空间使用状况，及时采取相应措施。

这些信息便于管理人员随时掌握系统内部使用情况，及时发现问题，提高系统性能。

此外，通过点击“关机”和“重启”按钮，可将 KILL Shield Gateway 系统关机或重启。这时会弹出对话框，要求用户确认。用户点击“确定”后系统关机或重启。

网络配置

在系统配置界面，点击“网络配置”进入到配置网络界面，在这里用户可根据自己网络的实际情况，进行 KILL Shield Gateway 的网络配置。可以看到，KILL Shield Gateway 支持多网卡结构，根据用户网络状况和需求，最多可使用 4 块网卡，如下图 3-3 所示。



图 3-3 KILL Shield Gateway 的网络配置

在“主机名”编辑框中输入 KILL Shield Gateway 所在机器的主机名称,使用 FQDN(Fully Qualified Domain Name) 名称,如 m5.ca-jc.com。

在“默认网关”编辑框中输入系统所在网络的默认网关。如 192.168.168.1。


如果采用多块网卡,则在“默认网关设备”中选择网关的设备名称。

下面对每块网卡配置 IP 地址。“eth0”代表第一块网卡,“eth1”代表第二块网卡,依次类推。

在“IP 地址”编辑框中输入 KILL Shield Gateway 系统所在机器使用的 IP 地址,如 192.168.168.5。

在“子网掩码”编辑框中输入系统所在网络的子网掩码。如 255.255.255.0。

通过在浏览器中进行这些设置,界面友好,无需用户手工输入相关命令,简化了用户操作。所有这些项在点击“确定”后才保存,并将在重启机器后生效。

关于每项输入的格式,还可查看在线帮助。方法是將鼠标移到编辑框右边的  图标上,这时会自动弹出对该项输入的帮助,包括输入内容、格式、要求等,使用户一目了然。

域名解析

点击“域名解析”进入到设置域名服务器的配置页面,缺省显示以前的配置结果,便于用户修改前参考。如图 3-4 所示。

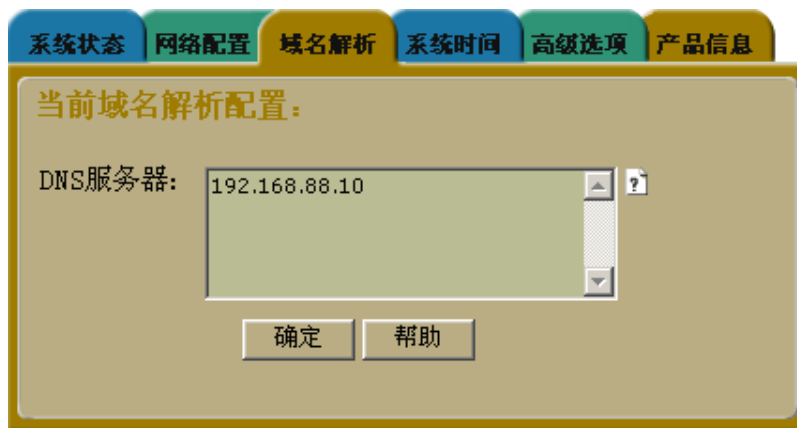


图 3-4 KILL Shield Gateway 的“域名解析”页面

在“DNS 服务器”中,输入域名解析服务器的 IP 地址,最多可输入 3 个 DNS 服务器地址,中间用回车符断开。当有多个服务器时,按照从上到下的列表顺序进行查询。

点击“确定”,将 DNS 配置保存,这时会在屏幕上显示“成功更新”,并在重启后生效。

系统时间

当要校准系统时间时，点击“系统时间”进入到设置系统时间的配置页面（如图 3-5）。

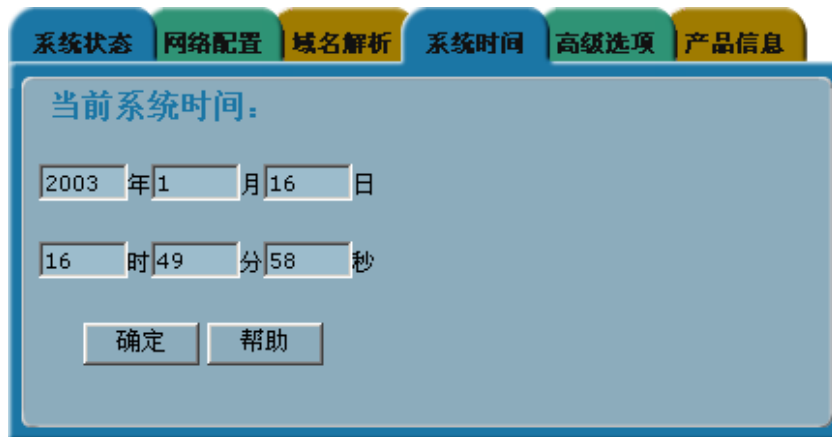


图 3-5 KILL Shield Gateway 的“系统时间”页面

用户只需在编辑框中输入修改后的系统时间，点击“确定”即可，该操作立即生效，屏幕上将显示“成功更新”。

高级选项

在“高级选项”中设置是否开启 SSH（即 Secure Shell），SSH 是一个用来替代 TELNET、FTP 等命令的工具，由客户端和服务端的软件组成，主要是想解决在网上明文传输的问题。通过使用 SSH，你可以把所有传输的数据进行加密，避免遭受类似“中间人”这类方式的攻击，确保传输内容的安全。（如图 3-6 所示）



图 3-6 KILL Shield Gateway 的“高级选项”页面

开启 SSH，即指启动服务端，为的是远程管理的方便，用户可根据自己情况判断是否需要开启该功能。点击“确定”后，屏幕上将显示“成功更新”，该操作立即生效。

产品信息

在“系统配置”页面，点击“产品信息”可查看产品的详细信息，包括产品型号、出厂日期、硬件型号、产品序号、软件版本等。这些信息便于用户了解产品情况，如遇到问题时

可向厂家提供这些信息，以利于问题的解决。

“用户管理”页面

点击主界面左边的“用户管理”按钮，进入到“用户管理”配置页面。该页面包括两大功能：更改管理员信息和更改口令。这些信息用于增强管理的安全性，发送报警通知及生成报表等。

对于单域产品（406 型号），一台机器只有一个管理员，负责 KILL Shield Gateway 的所有配置；对于多域产品（408 型号），有两种管理员，一是**超级系统管理员**，他能够对 KILL Shield Gateway 的所有域做所有设置，另一种为**域管理员**，他们登录后只能修改和本域相关的设置，修改自己的管理员信息和密码。

建议经常更新管理员的口令，以确保不会被未授权用户得到口令后恶意修改产品配置。

设置用户信息

首先进入“用户信息”页（如图 3-7）。缺省情况下将管理员的相关信息列出。

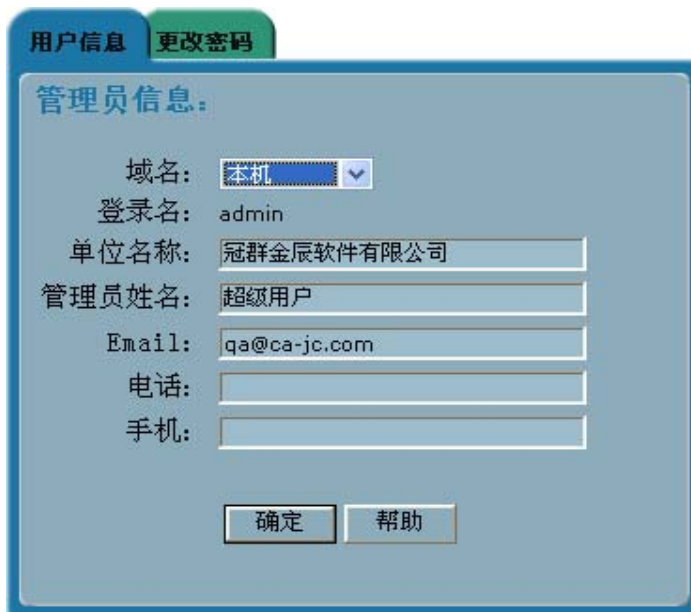


图 3-7 KILL Shield Gateway 的“用户信息”页面

对 406 型号（即单域）产品，域名、登录名直接显示在界面上，用户只能修改以下信息：

“单位名称” -- 输入使用 KILL Shield Gateway 的单位名称，用做报表信息。

“管理员姓名” -- 输入管理员的全名，中英文均可。

“Email” -- 输入管理员的邮箱地址，用于发现病毒后通知系统邮件管理员。

“电话”和“手机”-- 输入管理员的联系电话，以便发现问题后及时与管理员取得联系。

对 408 型号（即多域）产品，如果以超级系统管理员身份登录到管理界面，则可以选择要更改哪个域的管理员信息，其中“本地”指修改超级管理员自己的信息。如果是域管理员身份登录到管理界面，则只能修改本域信息。

点击“确定”保存这些信息，界面上将显示“成功更新”。

更改口令

为了使用上的安全性，防止未授权用户篡改邮件管理员已配置好的安全策略，在进入 KILL Shield Gateway 的管理页面前，必须输入管理员名称与口令。第一次进入管理界面时，可使用系统缺省建立的用户名和口令（用户名 admin，口令 killksg），进入到配置界面后，首先要做的就是修改管理员口令，否则就毫无安全性可言了。此外，在正常使用过程中，仍应定期更新管理员密码，以防密码被未授权用户通过不正当方式得到，恶意更改已定的安全策略，导致不必要的损失。

点击“更改口令”标签进入到修改管理员口令的界面（如图 3-8）。

图 3-8 KILL Shield Gateway 的“更改口令”页面

在“域名”中选择要更改哪个域的管理员密码。（406 型号直接列出该域）

在“登录名”中输入所选域的管理员的登录名称，可输入一个新的登录名。

在“原密码”项中输入该管理员的原登录密码。原登录密码必须正确输入时才可修改密码。否则，界面上显示“输入错误”，并视输入的新密码无效。只有超级管理员更改域管理员的密码时，不需提供原密码。

在“新密码”项中输入该管理员即将使用的新密码。为加强安全性，密码长度至少 6 位。

在“重输新密码”项中再次输入新密码，以确认用户输入密码无误。该项内容必须和上一项内容一致。否则会弹出警告框，如图示，并等待重新输入。



所有这些项在点击“确定”后才生效。此时屏幕上会显示“成功更新”。

选择一个好口令的建议

一个口令至少有 6 个字符长；

口令不应该是一个简单的单词或可从字典中查到的单词；

最好在口令中包含大写字母、小写字母和数字，例如 *Secret45*；

口令不应与登录名相似。

“过滤引擎”配置页面

在“过滤引擎”页面中，包括“病毒”、“关键字引擎”和“垃圾邮件引擎”三种引擎的设置页面。下面详细介绍。

病毒引擎

为确保 KILL Shield Gateway 能时刻查杀新病毒，在防病毒过程中，我们需要不断更新病毒特征码。该工作既可手动进行，也可自动进行。通常情况下，病毒引擎两三天左右更新一次。邮件系统管理员应设置策略定期进行最新的病毒特征码更新。

然而，不可预知的新病毒可能随时出现，并且防不胜防。对突发的病毒，KILL 还会立即升级，我们建议你规律地定期地查看我们的网站，尤其是当你听到有关新病毒的感染和攻击时。为了更好地保护你的计算机系统，请与冠群金辰公司的最新特征码保持一致。

在主界面上点击“过滤引擎”，然后点击“病毒”选项卡，进入到病毒引擎升级设置界面。在该界面中，设置 KILL Shield Gateway 的病毒引擎升级策略。如图 3-9 所示。



图 3-9 KILL Shield Gateway 的“病毒引擎”页面

在“特征码下载地址”栏中输入 KILL 的病毒库下载地址，缺省是从 <ftp://download.ca-jc.com/update/av> 下载。

在“下载时间”选项中选择每周的什么时间下载，KILL Shield Gateway 将根据设定的时间定时自动下载病毒特征码。建议在邮件系统空闲时进行病毒特征码的下载工作，以提高工作效率。

点击“确定”保存升级配置，系统将定期更新特征码，或者点击“立即下载”立即更新病毒特征码。

升级日志

点击“显示升级日志”按钮，可在屏幕上显示最近 15 天内的升级日志，包括 15 天内共升级几次，每次升级的时间、状态、版本及备注等内容，使邮件管理员及时了解病毒特征码的升级情况，确保对最新病毒的查杀工作。如图 3-10 所示。

15天内共升级 8 次			
日期	状态	版本	备注
2002-07-25 16:08:08	成功	23.56.10	您已经拥有当前最新的升级文件。
2002-07-25 16:08:01	成功	23.56.10	您已经拥有当前最新的升级文件。
2002-07-25 02:30:10	成功	23.56.10	升级成功。
2002-07-23 02:30:01	成功	23.56.06	您已经拥有当前最新的升级文件。
2002-07-22 02:30:16	成功	23.56.06	您已经拥有当前最新的升级文件。
2002-07-21 02:30:32	成功	23.56.06	升级成功。
2002-07-20 02:30:04	成功	23.56.04	升级成功。
2002-07-19 18:13:53	成功	23.56.01	您已经拥有当前最新的升级文件。

图 3-10 KILL Shield Gateway 的“升级日志”页面

点击“关闭升级日志”按钮，可关闭此页。

关键字引擎

对邮件除了可进行病毒过滤外，还可进行关键字过滤。

在主界面上点击“过滤引擎”，然后点击“关键字引擎”选项卡，进入到关键字过滤列表设置界面。如图 3-11 所示。



图 3-11 KILL Shield Gateway 的“关键字引擎”管理页面

在该页中设置关键字引擎的查找列表，缺省显示已定义的关键字。KILL Shield Gateway 的关键字过滤引擎查找邮件的主题、正文、附件名、文本附件中是否含有指定的关键字，一旦发现匹配，将丢弃该邮件，并根据关键字引擎过滤策略通知相关人员，防止敏感性信息通过邮件发送。

在“关键字”框中直接键入对邮件要监控的关键字，可输入多个关键字，中间用回车符断开。点击“确定”，屏幕上显示“成功更新”。这样，当 KILL Shield Gateway 检测到邮件中包含列表中任意一个条目时，将根据策略采取相应措施。

垃圾邮件

在主界面上点击“过滤引擎”，然后点击“垃圾邮件”选项卡，进入到关键字过滤列表设置界面。如图 3-12 所示。



图 3-12 KILL Shield Gateway 的“垃圾邮件”管理页面

KILL Shield Gateway 的垃圾邮件过滤引擎可检测两种格式的垃圾邮件过滤条件：电子邮件地址格式和主机名/地址格式，一旦发现匹配即丢弃该邮件，可输入多个垃圾邮件过滤条件，中间用回车符断开，只要符合其中之一则丢弃。由于是在未接收邮件前即丢弃，故不提供垃圾邮件过滤日志及通知相关人员。各种匹配格式说明如下：

- 电子邮件地址格式

包括以下具体形式：

user@domain 匹配指定的邮件地址。

domain.name 将 domain.name 作为 email 地址的域部分进行匹配。如对 company.com 匹配，来自 company.com 域的所有邮件将认为是垃圾邮件。domain.name 格式还可匹配该域的子域。

user@ 匹配所有的带有指定用户名部分的邮件地址。如在列表中输入Roxy@，则所有Roxy发送的（不管通过哪个邮件域转发的）邮件都将被认为是垃圾邮件。

- 主机名/地址格式

可采取主机名格式，如 ns.company.com，指定特定主机。也支持域名方式，如匹配 company.com 域，还可以用.domain.name(注意开始的点)匹配子域。

对地址格式，可采用 IP 地址形式指定要匹配的主机地址或网络，如键入 192.168.88.1 (指定主机 IP 地址)，192.168.88，192.168，192 等指定子网。

“邮件系统”页面

在主界面上点击“邮件系统”，可配置允许转发的 IP 地址范围和是否启用 SMTP 认证。如图 3-13 所示。



图 3-13 KILL Shield Gateway 的“邮件系统”配置页面

为了防止对 MTA 的滥用，许多 MTA 在接受邮件客户端的发信请求前，要求对其身份作认证，这就是所谓的 SMTP 认证。如果用户的邮件服务器要求邮件客户端进行认证，在引入了 KILL Shield Gateway 之后，客户端要求使用 KILL Shield Gateway 作为转发服务器，此时 SMTP 认证的过程将由 KILL Shield Gateway 来进行。KILL Shield Gateway 会将这一认证过程的数据流重新定向给用户的原邮件服务器，并根据认证的结果来决定是否接收客户端的发信请求。认证的过程完全遵循 ESMTP 的认证协议标准。

如果用户的原邮件服务器不支持 SMTP 认证但希望增加 SMTP 认证功能，可以启用 SMTP 认证，并使用 KILL Shield Gateway 的 SMTP 认证扩展模块（具体配置见“邮件配置”页面），这样用户就可以使用 KILL Shield Gateway 进行发信认证了。

在“邮件系统”界面，对转发邮件可有两个限制条件，只要满足了以下条件的任一个，就可通过 KILL Shield Gateway 转发邮件：

- 发件客户端 IP 地址符合“允许转发的 IP 范围”中设置的 IP 范围；
- 发件人是否通过 SMTP 认证（如果启用 SMTP 认证）；

KILL Shield Gateway 按先后顺序进行检查，一旦满足条件，则不再检查是否满足后面的条件，并开始按照设置进行邮件的转发与认证工作。

在“允许转发的 IP 地址范围”框中，直接输入可以使用 KILL Shield Gateway 进行邮件转发的 IP 地址范围，即在此范围内的客户 IP 地址可以使用此服务器发信，以“网络地址/子网掩码”的格式输入，例如 192.168.88.0/255.255.255.0。如要输入多个 IP 范围，则回车后再输入下一个子网地址。

在“启用 SMTP 认证”选项中，根据用户实际情况，判断 KILL Shield Gateway 是否启用 SMTP 认证功能。

“邮件域”页面

该管理页面只在 408 型号（多域）产品中可用，用来增加要保护的邮件域及对该域的一些控制，包括设定域名、域邮件服务器、域状态等。

增加新域

在此界面中，输入新的受保护域的信息，如图 3-14 所示。



图 3-14 KILL Shield Gateway 的“增加新域”页面

在“域名”中输入新的受保护域的域名，即指定 KILL Shield Gateway 接收邮件时收件人的域名，如 ca-jc.com。KILL Shield Gateway 可保护多个域的邮件免受病毒危害。

在“单位名称”栏中输入使用该域的单位名称，以便将来制作不同单位的邮件过滤报表。

在“邮件服务器地址”栏中输入该域的原邮件服务器地址。因为 KILL Shield Gateway 要先检查邮件是否带有病毒，处理后再将其发送给原邮件服务器，所以为保证邮件的正确接收，该地址务必写正确。

在“域状态”中，选择该域状态。其中，“激活”表示对该域 KILL Shield Gateway 提供

正常的病毒过滤保护功能,该域的用户可正常收发邮件,并可确保邮件是不包含病毒的;“禁用”表示该域不再可用,所有用户将无法使用 KILL Shield Gateway 转发邮件;“锁定”表示将病毒过滤功能暂停,用户仍可以正常收发邮件,但对该域不再提供任何安全保护。只有超级管理员才可执行此项设定。

在“记录过滤日志”选项中,指定是否要记录日志。日志用于将来查看邮件病毒情况,便于管理员采取相应措施。除非有特殊原因,如硬盘空间问题等,否则一般应启用日志功能。

“日志保存期限”:为节省硬盘空间,建议清除一定时间以上的日志文件。在这里指定日志保存期限后,KILL Shield Gateway 到时会自动清除日志。该值必须在 1 至 18 个月之间。如果在“记录过滤日志”项中选择不记录日志,则此项可以为空,表示保留原日志不变。

点击“确定”并经过滤网关检验所输信息合格后,屏幕上显示“成功添加新域”,同时增加“查看”按钮,用户点击该按钮便进入到“各域配置”界面,可查看已有各域的信息,检查刚才增加的域是否设置正确等。

重复上述步骤,可增加多个受管理的域。

各域配置

在本页面中显示各域配置情况,超级管理员还可对各域的配置进行编辑,并删除已存在的域。如图 3-15 所示。



图 3-15 KILL Shield Gateway 的“各域配置”信息页面

在“域状态”栏中,可更改各域的状态。参见“增加新域”一节中对域状态的解释。点击“确定”保存修改。

要删除一个域,直接点击该域右边的“删除”按钮,确认后即可。

对域的更多编辑工作,在点击该域名后进行。如点击上图中域名 test.com,进入到如图

3-16 所示页面，通过点击各超链接，进入各相关页面，可以分别修改该域的管理员信息和密码，设置该域邮件系统详细情况和病毒过滤策略等，查看过滤报表等。



图 3-16 编辑各域配置信息

“ 邮件传递 ” 页面

在主界面上点击“ 邮件传递 ”，进入到邮件系统收发配置界面。对于 408 型号，可为不同的邮件域做不同的配置。在这里配置 KILL Shield Gateway 的邮件系统的各种选项，确定其工作方式。

接收与传递

在“ 接收与传递 ”页中可设置、更改邮件服务器接收邮件的配置，缺省显示原配置。如图 17 所示。



图 3-17 KILL Shield Gateway 邮件系统的“ 接收与传递 ”配置

在“邮件域”中指定 KILL Shield Gateway 邮件系统要接收什么样的邮件，如 ca-jc.com。对于 408 型号，直接选择要更改配置的域名，对 406 型号，则直接输入要管理的邮件域。

在“该域的邮件服务器地址”编辑框中输入启用 KILL Shield Gateway 前该域使用的邮件服务器的 IP 地址。因为 KILL Shield Gateway 要先检查邮件是否带有病毒，处理后再将其发送给原邮件服务器，所以为保证邮件的正确接收，该地址务必写正确。

在“记录过滤日志”选项中，指定是否要记录日志。日志用于将来察看邮件病毒情况，便于管理员采取相应措施。除非有特殊情况，如硬盘空间问题等，否则一般应启用日志功能。

“日志保存期限”：为节省硬盘空间，建议清除一定时间以上的日志文件。在这里指定日志保存期限后，KILL Shield Gateway 到时会自动清除日志。该值必须在 1 至 18 个月之间。如果在“记录过滤日志”项中选择不记录日志，则此项可以为空，表示保留原日志不变。

点击“确定”，更新邮件系统的接收与传递配置，成功后页面上会显示“成功更新”，并立即生效。

发件认证

注意：只有在“邮件系统”页面中选择启用“SMTP”认证后，才会出现本页面。

为了防止对 MTA 的滥用，许多 MTA 在接受邮件客户端的发信请求前，要求对其身份作认证，这就是所谓的 SMTP 认证。如果用户的邮件服务器要求邮件客户端进行认证，在引入了 KILL Shield Gateway 之后，客户端要求使用 KILL Shield Gateway 作为转发服务器，此时 SMTP 认证的过程将由 KILL Shield Gateway 来进行。KILL Shield Gateway 会将这一认证过程的数据流重新定向给用户的原邮件服务器，并根据认证的结果来决定是否接收客户端的发信请求。认证的过程完全遵循 ESMTP 的认证协议标准。

如果用户的原邮件服务器不支持 SMTP 认证，可以使用 KILL Shield Gateway 的 SMTP 认证扩展模块，KILL Shield Gateway 有 POP3 协议的 SMTP 认证扩展模块，可以将 SMTP 认证协议转变为对 POP3 用户的认证协议，这样用户就可以使用 KILL Shield Gateway 进行发信认证了。

在“邮件配置”界面上点击“转发与认证”进入到转发限制设置页面，以防止垃圾邮件泛滥，工作效率降低。如图 3-18 所示。



图 3-18 KILL Shield Gateway 的“发信认证”页面

在“域名”中指定 KILL Shield Gateway 邮件系统要配置哪个域的发信认证模式，对于 408 型号，需选择要配置认证模式的域名，对 406 型号（单域产品），则直接显示被管理的邮件域。

在“认证模式”下拉列表中，选择认证模式。KILL Shield Gateway 的 406 和 408 型号都支持两种认证模式：SMTP 和 POP3。下面逐一介绍。

SMTP 模式

该模式用于用户原邮件系统具有 SMTP 认证的情况，启用 KILL Shield Gateway 后，它将用户认证信息转给原邮件系统的 SMTP 认证服务器，然后根据返回的信息判断是否转发邮件，以防垃圾邮件泛滥，增加邮件服务器的负担。在选择 SMTP 模式后，应在下面的“认证服务器地址”编辑框中输入 SMTP 认证服务器的 IP 地址，在“端口号”框中输入该服务器提供认证服务的端口号。一般来说，SMTP 认证采用 25 端口。

POP3 模式

针对用户邮件系统都具有 POP3 认证，但未必具有 SMTP 认证的情况，KILL Shield Gateway 提供了 POP3 模式的 SMTP 认证，即 KILL Shield Gateway 将用户认证信息转给原邮件系统的 POP3 认证服务器，然后根据返回的信息判断是否转发邮件。因此在选择 POP3 模式后，应在下面的“认证服务器地址”编辑框中输入 SMTP 认证服务器的 IP 地址，在“端口号”框中输入该服务器提供认证服务的端口号。一般来说，POP3 认证采用 110 端口。

点击“确定”保存配置。

“邮件过滤”配置页面

在主界面上点击“邮件过滤”，进入到过滤策略设置界面，包括病毒过滤策略和关键字

过滤。

病毒过滤策略

在“病毒”页中，显示以前制定的病毒过滤策略，邮件管理员可根据实际情况进行修改，如图 3-19 所示。对 408 型号，不同的邮件域可以有不同的策略，即可选择一个域名后设置策略。对 406 型号，要配置病毒过滤策略的域名直接显示在界面上。



图 3-19 KILL Shield Gateway 的病毒过滤策略

邮件管理员可修改以下选项：

过滤范围：选中“接收邮件”表示从外部发向该域的邮件启用反病毒引擎，选中“发送邮件”表示从该域发向外部的邮件启用反病毒引擎，或者二者皆选。如果二者皆不选，则 KILL Shield Gateway 只是简单的将邮件转发，不进行任何邮件查杀毒工作。

通知管理员：选择该项后，发现病毒邮件时，KILL Shield Gateway 将发送病毒通知给管理员，管理员邮箱是在“用户管理”页中指定的。

通知发件人：在发现病毒邮件后，选择该项 KILL Shield Gateway 将发送病毒通知给发件人，以便发件人及时采取查杀毒措施，从而达到减少病毒邮件的来源的目的。

发现病毒后所采取的操作：如果选用“清除病毒”，KILL Shield Gateway 将尝试修复染毒的附件，如因种种原因（如文件已被病毒损坏等）造成修复失败，则根据下面“清除失败后所采取的操作”选项的设置对邮件进行处理。如果选择“删除附件”则 KILL Shield Gateway 不尝试修复染毒附件，而直接将染毒附件删除。这在工作负荷较大时有助于提高查杀毒效率。如果选择“丢弃邮件”，则 KILL Shield Gateway 将直接将该邮件完全丢弃，并发一封信通知给相关人员。

清除失败后所采取的操作：当发现病毒后所采取的操作为“清除病毒”时，在这里选择如果清除病毒失败应采取的操作，包括删除附件和丢弃邮件两种。

所有这些选项在点击“确定”后被保存，并可立即生效。

关键字

在“邮件过滤”页中，点击“关键字”选项卡，设置对邮件中关键字的过滤策略。如图 3-20 所示。



图 3-20 KILL Shield Gateway 的关键字过滤策略

过滤范围：选中“接收邮件”表示从外部发向该域的邮件启用关键字过滤引擎，选中“发送邮件”表示从该域发向外部的邮件启用关键字过滤引擎，或者二者皆选。如果二者皆不选，则 KILL Shield Gateway 只是简单的将邮件转发，不进行任何关键字过滤工作。

通知管理员：选择该项后，发现匹配关键字列表的邮件时，KILL Shield Gateway 将发送病毒通知给管理员，管理员邮箱是在“用户管理”页中指定的。

通知发件人：在发现匹配关键字列表的邮件后，选择该项 KILL Shield Gateway 将发送病毒通知给发件人，从而达到减少此类内容邮件的来源的目的。

所采取的操作：针对匹配关键字的邮件，KILL Shield Gateway 将直接丢弃该邮件，保证收发邮件内容的合法性，同时会根据上面的策略通知相关人员。

“邮件报表”页面

在主界面上点击“邮件报表”按钮，进入到生成、查看邮件过滤报表界面，可查看两个引擎过滤邮件情况的报表：病毒报表和关键字报表。

对病毒引擎，KILL Shield Gateway 可提供五种报表，以满足用户的不同需求，它们分别是病毒邮件比例报表、内部带毒邮件账户报表、外部带毒邮件账户报表、病毒邮件时段分布报表和病毒邮件趋势报表。

对关键字引擎，也是提供五种报表，分别是：关键字邮件比例报表、内部关键字邮件账户报表、外部关键字邮件账户报表、关键字邮件时段分布报表和关键字邮件趋势报表。由于两种引擎报表结构相似，下面以病毒引擎报表为例介绍各报表的内容。

单击主页面“邮件报表”按钮，然后点击“病毒报表”选项卡，进入病毒报表的生成、查看页面。如图 3-21 所示。

图 3-21 KILL Shield Gateway 的病毒报表生成页面

报表的时间范围是从起始日的零点到终止日的 24 点。考虑到方便用户查看，这些报告都采用形象的图表式结构，使邮件管理员一目了然，及时了解网络中邮件病毒的发作情况。

- 病毒邮件比例报表

病毒邮件比例报表显示一定时间内，KILL Shield Gateway 收到的邮件总数，收到的带病毒邮件的总数及所占比例，收到病毒邮件中十种最多的病毒，发出邮件总数，发出病毒邮件总数及比例，发出病毒邮件中十种最多的病毒等，以形象的图表结构提交给用户。管理员可了解收发的邮件中主要包含哪些病毒，从而可采取相应措施。

在“病毒报表”页面，从“报表类型”下拉列表中选择“病毒邮件比例报表”，并输入统计的起始时间和终止时间，点击“确定”，显示生成的报表。

- 内部带毒邮件账户报表

该报表显示一定时间内，从局域网中发出病毒邮件数量最多的前 10 名用户邮箱，以及

通过这些邮箱发出的染毒邮件总数和数量最多的前三位病毒,管理员通过此报表可了解到网络中哪些用户的计算机系统病毒感染较严重,从而采取相应措施。

在“病毒报表”页面,从“报表类型”下拉列表中选择“内部带毒邮件账户报表”,并输入统计的起始时间和终止时间,点击“确定”,显示生成的报表。

- 外部带毒邮件账户报表

该报表显示一定时间内,从外部网络发入病毒邮件数量最多的前 10 名用户邮箱,以及通过这些邮箱发出的染毒邮件总数和数量最多的前三位病毒,管理员通过此报表可了解到外部网络中哪些用户经常发送带毒邮件,从而采取相应措施。

在“病毒报表”页面,从“报表类型”下拉列表中选择“外部带毒邮件账户报表”,并输入统计的起始时间和终止时间,点击“确定”,显示生成的报表。

- 病毒邮件时段分布报表

时段报表显示一定日期内,每时段收到邮件数量,收到病毒邮件数量及所占比例,每时段发出邮件数量,发出病毒邮件数量,以形象的图表结构提交给用户,管理员可迅速发现病毒邮件的高峰期,采取适当措施,确保邮件系统的安全。如图所示。

- 病毒邮件趋势报表



图 3-22 KILL Shield Gateway 的病毒邮件时段分布报表

该报表显示在选定的日期范围内，每天收到的邮件数，收到的带病毒邮件数，收到病毒邮件比例，发出的邮件数，发出的带病毒邮件数，发出病毒邮件比例等。通过此报表，管理员可了解到系统的病毒发作趋势，可根据此趋势确定反病毒的工作成效。

在“病毒报表”页面，从“报表类型”下拉列表中选择“病毒邮件趋势报表”，并输入统计的起始时间和终止时间，点击“确定”，显示生成的报表。

注意：

KILL Shield Gateway 还定期（每个月初）将这些报表发送给邮件系统管理员，以便管理员掌握邮件系统的使用情况及用户的病毒发作情况，确保邮件系统的安全。同时，为确保管理员能收到邮件，在每月的15日还将重发此邮件。

管理员将收到主题为 report by time 的邮件，含有五个超链接，分别指向比例报表、内部邮箱报表、外部邮箱报表、时段报表和趋势报表，用户收到邮件后，只需点击列出的某项链接，便可查看相关报表。

“退出”页面

当管理员修改完配置后，建议点击“退出”按钮退出管理界面，防止没有管理员权限的人对已做好的配置进行修改，提高产品使用的安全性。为防止误操作，KILL Shield Gateway 将询问是否确定要退出。如图 3-23 所示。



图 3-23 KILL Shield Gateway 退出确认

退出后返回到登录界面，如图 3-24 所示。等待合法用户登入管理界面。



图 3-24 KILL Shield Gateway 的登录界面

在“用户名”中，输入该系统的合法用户名。

在“密码”中，输入该用户的密码。


点击“确定”，如果上述信息均正确，则可直接进入到管理界面，否则，屏幕上显示：

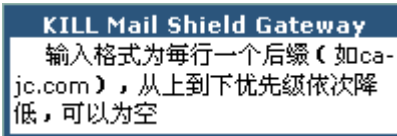
登录失败，请重试！

从而确保只有授权用户可以登录到管理界面。

KILL Shield Gateway 的帮助文档

为便于用户使用，KILL Shield Gateway 为提供多种方式的帮助及相关文档。包括：

在线帮助：在管理界面的每项需用户选择或输入的项后，都有一个问号  图标，用户只需将鼠标移到该图标上，会自动弹出对该项输入的帮助，包括输入内容、格式、要求等，使用户一目了然。（如图）



帮助文件：在每个管理界面上，都有一个“帮助”按钮，点击该按钮，可浏览如何管理 KILL Shield Gateway 的帮助文件，该文件对每项都有详细的解释。

用户手册和白皮书：随产品还提供了用户手册及白皮书，用户可从中找到关心的技术问题及解决办法。

第四章 KILL Shield Gateway 使用举例

用户网络环境概述

用户目前只有一个邮件域 domain.com。用户的邮件服务器、DNS 服务器等服务器均位于局域网中的 DMZ 区，受到防火墙的保护。防火墙通过地址映射功能，将邮件服务器的 Internet 地址映射到邮件服务器的内部地址。具体配置如下所示。

原配置为：

参数名	参数值

要保护的邮件域	domain.com
该域原有邮件服务器的 IP 地址及名称	内部 192.168.1.1 外部 202.1.1.1 mail.domain.com 别名 pop3.domain.com smtp.domain.com
内部 DNS 服务器的 IP 地址	192.168.1.3
网关地址	192.168.1.254
是否支持 SMTP 认证	是，认证服务器即邮件服务器 192.168.1.1
原邮件客户端发件服务器配置	smtp.domain.com
原邮件客户端收件服务器配置	pop3.domain.com

为 KILL Shield Gateway 分配的参数为：

KILL 过滤网关域名	smtp.domain.com
KILL 过滤网关的 IP 地址	内部 192.168.1.2 外部 202.1.1.2

操作步骤

首先将 KILL 过滤网关连接到网络的 DMZ 区中，然后执行下述步骤：

一、系统配置

1、网络配置

进入到 KILL Shield Gateway 管理界面，“基本系统”-“网络配置”，设置该机器的主机名 smtp.domain.com、IP 192.168.1.2、网关 192.168.1.254 等内容。

2、域名解析配置

在“基本系统”-“域名解析”中，输入 DNS 服务器 IP 192.168.1.3。

配置完成后重启 KILL Shield Gateway。

二、邮件系统配置

1、启用认证

在 KILL 过滤网关的管理界面上，单击“邮件系统”，选择“启用 SMTP 转发认证”为“是”。启用认证后的具体配置见步骤 3 所述。

2、接收与传递

在管理主界面上，点击“邮件传递” - “接收与传递”，指定邮件域为 *domain.com*，邮件服务器地址为 192.168.1.1。单击“确定”保存配置。

3、转发与认证

在管理主界面上，点击“邮件传递” - “转发认证”，指定采用 SMTP 认证，认证服务器即原邮件服务器，输入 192.168.1.1。单击“确定”保存配置。

三、设置过滤策略

在管理界面中进入“邮件过滤”，进入到邮件过滤策略设置界面。该操作较简单，不多讲了。

四、测试

原邮件客户端的收发邮件服务器分别为 *smtp.domain.com* 和 *pop3.domain.com*。

现将邮件客户端发邮件服务器改为过滤网关的 IP 地址 192.168.1.2，收件服务器地址不变。

用一个该邮件域的测试用帐户，给自己发封信，确认通过 KILL 过滤网关可正常收发信。否则请检查前面的配置。

五、修改内部 DNS 后测试

确保使用过滤网关的 IP 可正常收发邮件后，就可以修改内部 DNS，将 *smtp.domain.com* 的 IP 地址改为过滤网关的 IP 地址，即 192.168.1.2。可用 `nslookup` 命令确认 DNS 的修改已生效。

将邮件客户端的收件服务器的发件服务器改为 *smtp.domain.com*，（注意此时 *smtp.domain.com* 实际上已指向 KILL 过滤网关）。收件服务器保持 *pop3.domain.com* 不变。通过邮件客户端进行收发邮件测试，确保可正常收发邮件。

六、修改外部 DNS 和防火墙设置。

1、修改外部 DNS

在 DNS 中为邮件域 domain.com 增加一条 MX 记录，优先级要高于原邮件服务器的优先级。

如原 DNS 为：

```
domain.com    IN  MX  10  mail.domain.com.  
mail.domain.com.  IN  A   202.1.1.1  
smtp.domain.com.  IN  A   202.1.1.1  
pop3.domain.com.  IN  A   202.1.1.1
```

现改为：

```
domain.com    IN  MX  10  mail.domain.com.  
domain.com    IN  MX  5   smtp.domain.com.  
mail.domain.com.  IN  A   202.1.1.1  
pop3.domain.com.  IN  A   202.1.1.1  
smtp.domain.com.  IN  A   202.1.1.2
```

可用 nslookup，dig 等命令确认已成功修改该域的 DNS 内容。

2、更改防火墙配置

在防火墙中增加一个地址映射，到 202.1.1.2 的 25 端口请求映射到过滤网关的内部 IP 192.168.1.2，反之亦然。

六、测试。

1、利用本域邮箱向外域，如 sina.com 的邮箱发送邮件，确保收发邮件正常，并可从邮件的属性看到该邮件经过了 KILL 过滤网关的过滤。

注意：所有过滤的邮件的属性中，都有“X-KILLShieldGateway-Checked”的标记。

2、从外域的邮箱向受保护的本域一个邮箱发送邮件，确保收发邮件正常，并可从邮件的属性看到该邮件经过了 KILL 过滤网关的过滤。

注意：由于一般邮件服务器都有缓存，所以即使 DNS 已经生效了，从外部邮件域发来的邮件仍有可能暂时不经过滤网关，当过了其 Cache 的刷新周期后，就可以按照 DNS 中的优先级，将邮件先发送到过滤网关，处理后再发给原邮件服务器了。

3、从本域的一个邮箱向本域另一个邮箱发送邮件，确保收发邮件正常，并可从邮件的

属性看到该邮件经过了 KILL 过滤网关的过滤。

常见问题解答

- KILL 过滤网关的病毒查杀能力如何？

KILL 过滤网关采用 KILL 的强大的反病毒引擎，经国际计算机安全协会认证对常见病毒（virus in-the-wild）能够 100%的快速有效清除。

- KILL Shield Gateway 产品如何进行特征码的升级？

用户可以预定时间从 <http://download.ca-jc.com/update/av> 网站自动获取最新的病毒定义特征码文件，也可手动更新。

- 建议什么时间执行病毒特征码自动升级？

建议在夜里访问较少的时间执行病毒特征码升级任务，而且每周至少选取两天定期更新。

- 我们使用的是 408 型号过滤网关，为什么选择认证方式后，发信时总提示认证不过去？

答：由于 408 型号为针对多域产品的网络过滤产品，所以当选择了使用发信认证（SMTP 认证）后，应注意在邮件客户端的账户信息中，输入账号的全称，如 admin@domain.com，而不是仅仅输入账户名。

- 如何查询扫描结果？

KILL Shield Gateway 针对扫描结果，可提供多种报表，用户可通过各种报表查看相关扫描结果，以了解邮件传输的安全情况。

- KILL 过滤网关是否可以进行关键字过滤和垃圾邮件过滤？

KILL 过滤网关可以进行上述过滤，详细内容请参见说明书中的描述。

- KILL 过滤网关是否可以同 web mail 配合工作？

KILL 过滤网关是否可以同 web mail 配合工作关键在于 web mail 的实现方式，具体的内容需要同负责 web mail 的厂家讨论才能确定。

- 发现病毒后 KILL 过滤网关如何通知给相关人员？

在配置 KILL 过滤网关时，可配置是否通知发件人和管理员，这样当过滤网关发现病毒

并进行处理后，将向收件人、发件人（根据用户选择）、管理员（根据用户选择）发送报警邮件，告知染毒的邮件、收件人、发件人、采取的措施等。

- 为什么通过直连方式更改过滤网关的 IP 地址后重启时有时会比较慢？

这与网卡有关，建议在重启前将直连线断开，这样过滤网关启动时不必再尝试与刚才连接的网卡进行连接（更改 IP 后与连接的网卡可能已不能连通），从而大大提高启动速度。

- 多域产品中的域状态：激活、锁定、禁用都表示什么意思？

“激活”表示对该域 KILL Shield Gateway 提供正常的病毒过滤保护功能，该域的用户可正常收发邮件，并可确保邮件是不包含病毒的；“禁用”表示该域不再可用，所有用户将无法使用 KILL Shield Gateway 转发邮件；“锁定”表示将病毒过滤功能暂停，用户仍可以正常收发邮件，但对该域不再提供任何安全保护。只有超级管理员才可执行此项设定。