

## KILL MailShield Gateway 赤霄 KILL 邮件过滤网关

随着计算机网络的飞速发展和应用,电子邮件系统已成为现代企业和广大用户进行通信与信息交流的主要手段,它在方便信息交流的同时,又为病毒提供了一个感染和快速传播的捷径,成为目前最常见的病毒传播途径。因此对各种邮件系统进行病毒防护,是当前防病毒厂家面临的巨大挑战。

但是邮件系统多种多样,不同的邮件系统需要不同的防毒软件,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毒软件。此外,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。

KILL MailShield Gateway 是一种与邮件系统类型无关的邮件防病毒产品,它解决了上述问题。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。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,并在查杀病毒的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。使用 KILL MailShield 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、自动生成报表,时时刻刻保护您的邮件系统。



KILL MailShield Gateway 的外观

### 友好的系统管理界面

KILL MailShield Gateway 的配置管理采用 B/S 方式,用户可使用浏览器远程查看、修

改 KILL MailShield 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。(如图示)



KILL MailShield Gateway 的系统信息界面

### 卓越的病毒查杀能力

KILL MailShield Gateway 的反病毒引擎获得了 ICSA(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。该引擎还凭借其卓越的病毒查杀功能荣获“Virus Bulletin”(病毒公告牌)授予的“VB 100%”奖,这是自 1998 年设立该奖项以来,该引擎第 19 次获得此殊荣,这一成就超过其它任何一个反病毒厂商。

### 更高的查杀毒效率

KILL MailShield Gateway 使用独立的硬件平台进行病毒的查杀工作,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 MailShield Gateway 的接入方式非常简单,无须修改原邮件服务器的任何配置,只要对本身和 DNS 进行简单的设置后,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 MailShield Gateway，从而保护用户的已有投资。

### 实时查杀病毒及报警

KILL MailShield 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，以便采取措施，保证邮件系统的安全。

### 多种病毒处理方法

KILL MailShield Gateway 对检测出含病毒的邮件有多种处理方法，可根据用户的设置进行修复、删除、报告等操作，如果操作设为修复，一旦修复失败 KILL MailShield Gateway 将删除染毒附件，以确保邮件安全。

### 病毒特征码的自动升级

KILL MailShield Gateway 可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。(如图示)



病毒特征码的升级配置

### 丰富的报表

KILL MailShield 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
- \* 发出病毒邮件用户统计报表
- \* 病毒时段分布报表(如图示)
- \* 病毒活动趋势报表

除了可自由选择报表统计的时段外，KILL MailShield Gateway 还在每个月初自动将上月报表发给管理员。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。



KILL MailShield Gateway 的病毒时段分布报表

### 强大的多域管理

针对大型企业，ISP 和 ASP 的邮件系统常常使用一个或多个 MTA 对多个域提供服务的情况，KILL MailShield Gateway 采用多域管理模块，可同时支持对多个域的邮件病毒过滤。使用集群模块时，还可使用多台 KILL MailShield Gateway 保护多个域的多个 MTA。

### 完善的自保护机制

KILL MailShield Gateway 设计有软件 WatchDog 和资源监测模块，具备自维护能力。当系统繁忙时，KILL MailShield Gateway 会将新收到的邮件放入缓冲队列，待系统空闲后再做处理。当 KILL MailShield 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。

### 支持 SMTP 认证

KILL MailShield Gateway 支持 SMTP 认证，防止垃圾邮件泛滥等滥用邮件系统的行为，保护正常用户发送的邮件不受干扰。认证过程完全遵循 ESMTP 的认证协议标准。即使原邮件系统未采用 SMTP 认证，仍可以使用 KILL MailShield 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，从而可使

用 KILL MailShield Gateway 进行发信认证。  
(如图示)



KILL MailShield Gateway 的邮件系统配置

### 过滤引擎扩充

KILL MailShield Gateway 的过滤引擎是可以扩充的，除了基本的病毒过滤引擎外，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 MailShield 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 MailShield 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 MailShield 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 MailShield Gateway 实现自动负载均衡，并通过集群模块，使各 KILL MailShield 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。