第9章 CHAPTER 构建可用的反垃圾邮件系统

前面已经介绍了多种反垃圾邮件的方法。但简单地将这些方法堆砌在一起，并不一定能够取得良好的反垃圾邮件效果。本章将介绍如何构建一个可用的反垃圾邮件系统。

9.1 各种方法的协同

多种保证邮件安全的算法，包括反垃圾算法和反病毒算法等，在系统中存在协同问题。同时，各种网络安全设备之间也存在协同问题。例如，当垃圾邮件和病毒邮件大量泛滥时，应该凭借防火墙分流，将邮件流量交由邮件安全系统处理，而将非邮件流量交 IDS 监控，否则大量的邮件流量会淹没 IDS，甚至导致 IDS 死机。

优化的引擎控制流程如下。

(1) 动态引擎-同时连接数控制：动态控制引擎的同时连接数控制模块在网络层限制大量同一 IP 的 SMTP 连接，并可能阻挡未知病毒和垃圾的泛滥程度。

(2) 病毒引擎：高效的病毒引擎发现所有已知病毒，可降低大量的病毒邮件对系统的冲击。

(3) 动态引擎-重复控制：动态控制引擎的用户重复、邮件重复和连接频率 3 个重复控制引擎限制同一发件人、同一主题、同一 IP 地址的邮件的发送频率，并可能阻挡未知病毒和限制垃圾邮件的泛滥程度。

(4) 垃圾引擎-黑白名单：垃圾引擎的黑白名单将已知的垃圾邮件发送者摒弃、放进已知的非垃圾发送者，黑白名单匹配的项不会再做其他垃圾检测工作。

(5) 垃圾引擎-可追查检查：垃圾引擎的可追查性检查高效地发现伪造了来源和路由

的邮件，这样的垃圾邮件占所有垃圾邮件的95%以上，阻挡的同时降低了高负荷的内容过滤和智能垃圾分析所需要的系统资源要求。

(6) 垃圾引擎-智能检测-智能RBL：智能RBL将这些黑名单列入的匹配邮件(注意，不仅是最早的RBL的IP地址列表)判断为垃圾邮件。

(7) 内容过滤引擎：产品模式内容过滤引擎发现内容匹配的邮件，主要针对政治、色情邮件，这些邮件一般不会再发给垃圾智能检测去分析或让贝叶斯过滤器去学习。

(8) 垃圾引擎-智能检测-贝叶斯/集中分析/内容分析/降噪：最后，上述方法都认为是正常的邮件经过负荷要求最高、但人工智能因素也最高的邮件特征智能集中分析和产品模式智能内容分析来判断该邮件是否是垃圾邮件，同时提交贝叶斯过滤器学习。相辅相成地，贝叶斯过滤器也可以判断该邮件是否是垃圾邮件，如果认为是，会自动提交智能集中分析服务器，同时智能降噪系统降低突发因素导致误判的可能。

低负荷、高性能、高准确性的防病毒引擎和可追查性检查引擎排除了绝大部分非正常邮件，使进入高负荷的智能检测引擎和较高负荷的内容过滤引擎的邮件量只占全部邮件的5%，相当于使整个系统的性能提高了20倍。

由于基于内容分析的反垃圾邮件方法占用相对多的系统资源，因此一台平时负荷不大、完全满足应用的邮件安全产品可能在邮件病毒爆发或垃圾邮件极度泛滥时系统资源被充满，自身防护不好的邮件安全产品甚至可能导致自身崩溃，因此在这时可以关闭高负荷的反垃圾邮件引擎，只使用负荷最低的可追查性检查，仍然能保证较好的反垃圾邮件效果。

9.2 工作模式

邮件安全产品依据其运行状态和与网络、网络中其他设备的连接方式，大致可以归结为3种运行模式：网关模式、MX转发模式和独立模式。其中，网关模式是指物理上与被保护的邮件服务器串联，转发模式是指物理上与被保护的邮件服务器并联，而独立模式是指在物理上与被保护的邮件服务器合并。

但要注意的是，这个分类并非很完善。物理上的并联可能在某种方式下形成逻辑上的串连。

1. 网关模式

在网络连接中，作为网关模式，可以有透明网关(网桥)、路由、应用网关3种实现，分别对应TCP/IP的第二层、第三层和第四层。

由于邮件服务是第四层的服务，因此实际上网关模式是对外的表现，而在产品中，必

然是从第二层或第三层上升到第四层处理，然后将数据包转发出去。

网关模式的反垃圾邮件产品可以完全保护邮件服务器，不会被垃圾邮件发送者短路，也不会让被保护的邮件服务器直接向外发送邮件而不通过反垃圾邮件产品。

网关模式唯一的缺点是：由于拓扑结构是“物理串联”，增加了一个故障点，即如果网关模式的反垃圾邮件产品发生故障，将导致邮件无法收发，这是用户有时不想使用网关模式反垃圾邮件产品的唯一可能原因。

透明网关模式的产品在使用上最为简便，无需修改原来邮件服务器的任何配置，只需要正确配置反垃圾邮件产品本身即可。透明网关在网络中的角色是网桥，是第二层的设备。

支持路由的网关模式产品初看起来可以保护邮件服务器无法被互联网直接访问，但实际的效果和透明网关相同。支持路由实际上相当于集成了部分简单路由器的功能，在邮件服务器处于内部网络同时需要对外连接时，有一定的用处，但可以靠透明网关和路由器实现相同的需求，因此路由模式意义不大。

邮件服务本身是第四层应用（网关）。

2. MX 转发模式

MX 转发模式在两个前提下可以保证冗余，即能够在邮件安全产品（MX 转发模式）故障时仍能收发邮件（只是丧失了反垃圾功能）。

- 邮件域 DNS 设置有两个不同优先级的 MX，高优先级指向反垃圾邮件产品，低优先级指向被保护邮件服务器。
- 邮件服务器和反垃圾邮件产品都能被互联网上的计算机访问到。

但是 MX 转发模式的缺点是能够被垃圾邮件发送者短路，垃圾邮件发送者可以直接将垃圾邮件送入被保护邮件服务器。同时，如果被保护邮件服务器不设置把发出的邮件送交反垃圾邮件产品转发，就会直接将邮件送出，导致本地可能会发出垃圾邮件或病毒邮件。

如果要回避这个缺点，可以取消邮件服务器的 DNS 设置，并用防火墙保证互联网无法直接访问邮件服务器、邮件服务器只能接收邮件安全产品转发的邮件，并配置邮件服务器将外发邮件首先转发给邮件安全产品。

但是这样调整后，网络拓扑就变成了“逻辑串联”，丧失了冗余的优势，和网关模式没有区别了。

3. 独立模式

独立模式，或者一些针对邮件服务器软件（或操作系统）的软件反垃圾邮件产品，将反垃圾邮件等邮件安全功能与邮件服务器合并，形成独立的、安全的邮件服务器。

9.3 提升系统性能

邮件安全产品是一个存在大量内容分析的产品，比网络层安全产品，例如防火墙，会消耗更大的负荷。如何提升邮件安全产品的性能，是必须考虑的问题。

邮件安全产品在正常使用时和在病毒邮件、垃圾邮件泛滥时的负荷是有极大差距的。因此，在病毒邮件和垃圾邮件泛滥时，如何保护邮件安全产品自身不会因为处理量过大而瘫痪，是一个必须考虑的问题。

9.3.1 双机热备

双机热备是保证系统可用性的重要方法。顾名思义，双机热备系统通常由两台运行相同服务的计算机组成，这两台计算机互为备份，而一般情况下只有一台计算机处于服务状态，另一台则处于同步备份状态。如果提供服务的计算机由于某种原因无法正常工作，备份机就立刻接管转换为服务状态，继续提供服务。这样就可以保证系统在一台计算机出现故障的情况下仍然可以正常运行。按照这样的原理，可以将双机热备系统扩展为三机、四机乃至更多计算机组成的热备系统，以提供更高的可用性。

对反垃圾邮件系统进行双机热备，同样可以提高系统在高负载情况下的可用性。

9.3.2 负载均衡

负载均衡也是在高负载情况下提供系统处理能力的常用方法。它通过将负载按照特定的规则分散到多个处理机中分别进行处理，这样单台处理机上的负载就会降低。在我们的反垃圾邮件系统中，可以使用四层交换机，将邮件流量分流到若干邮件安全产品。

使用 DNS 进行负载均衡是一个较简单而成本低廉的方式，具体方法为：

(1) 方法合理协同邮件安全产品使用 MX 转发模式，每台服务器有一单独的 IP 地址。

(2) 邮件域的 DNS 设置多个具有相同优先级的 MX 项。

(3) 如果需要全保护，将被保护的邮件服务器用防火墙配置为只接收来自邮件安全产品的连接。

这样，当发件服务器请求收件域 DNS 服务器时，会随机得到各台运行邮件安全产品服务器的 IP 地址，将邮件相对平均地发送到每台运行邮件安全产品服务器，从而得到较

高的性能。

9.3.3 方法合理协同

从理论上讲,组成反垃圾邮件系统的各反垃圾邮件子系统之间并没有太大的耦合性,因此在进行垃圾邮件分析判断时,邮件可以按照任意的次序来通过各子系统而不会影响最终的处理结果。但是,由于各个子系统对垃圾邮件的处理和限制能力不同,处理计算所需要的资源量也不同,如果能够合理安排和优化反垃圾邮件系统中各反垃圾邮件子系统处理的步骤和流程,尽早地在处理过程中鉴别出垃圾邮件,就可以有效降低信件平均处理时间,提高系统的整体处理能力。

例如,如果从某 IP 地址发出的邮件流量异常的高,那么不需要后面的各项垃圾邮件判断就可以断定,该 IP 地址正在发送垃圾邮件。因此,直接将网络层流量限制模块放在整个反垃圾邮件系统处理流程的第一步,就可以有效地提高反垃圾邮件系统处理大负载的能力,特别是提高对付 DoS 攻击的能力。

再如,如果一封邮件无法通过可追查性检查,即邮件的发件人地址经过伪装,那么已经可以肯定这就是一封垃圾邮件了,也就没有必要再进行反病毒检查等处理。这样也可以减少垃圾邮件处理所占用的资源。

总之,通过合理安排各个反垃圾邮件子系统的工作次序,可以有效提升系统的工作效率和性能。

9.3.4 反 DoS 攻击

由于邮件安全产品基本上是应用层的技术,因此没有自我保护的邮件安全产品在受到大量 SMTP 连接冲击时,首先表现为 SMTP 连接难以建立,其次可能导致应用层崩溃、SMTP 连接根本无法建立。在这时,除了提高系统性能,必须做的事首先是保护应用层不崩溃,其次是在应用层崩溃时,保证邮件正常收发。

1. 应用层保护

应用层保护的主要方法是限制整个邮件安全系统的最大并发连接数,限制单 IP 地址的最大并发连接数等。保护内存分配也可以起到一定的作用。

2. 保证邮件正常收发

在邮件安全产品应用层崩溃后,可以考虑两种方式保证邮件收发。但这里要先强调

的是：如果大量的 SMTP 连接冲击导致了邮件安全产品应用崩溃，而又通过某种方法保证邮件收发，很可能导致这大量的 SMTP 连接直接冲击被邮件安全产品保护的邮件服务器，进而导致邮件服务器崩溃。

MX 转发模式的邮件安全产品应用层崩溃时，如果邮件域的 DNS 设置了被保护邮件服务器为低优先级 MX 项，则发件服务器会自动将邮件直接向邮件服务器发送，这时所有的 SMTP 连接将冲击被保护邮件服务器。

下面说的两个保护方法是透明网关模式的邮件安全产品，但同样存在直接冲击被保护邮件服务器的问题。

- 网络层保护：一台 P4 级的计算机的二层或三层的 throughput 能保证上百 MB 的线速，因此即使应用层崩溃，核心层也不会崩溃，并且能保证所有流量线速转发。但一般的透明网关将 SMTP 数据截收给应用层，因此应用层崩溃时 SMTP 连接无法建立，所以需要一个核心层或硬件级的 WatchDog，接收来自应用层的 Reset，当应用层崩溃时，WatchDog 因无法接收 Reset 而超时，超时后核心层就不再将 SMTP 转到应用层处理，而是直接转发给邮件服务器。
- 硬件保护：硬件保护的方法很简单，实际上是将 WatchDog 做成一个硬件，接收来自邮件安全产品的 Reset，当邮件安全产品崩溃或硬件损坏导致 Reset 无法发出时，该硬件即将内外两个网口物理短路直通，保证网络继续能够通信。

可以看出，上述方法均是在邮件安全产品崩溃时试图保证邮件服务器能够继续直接和互联网通信，但这样导致大量 SMTP 连接直接冲击邮件服务器，有可能导致邮件服务器被冲垮或崩溃。从应用负荷上说，邮件安全产品处理每封邮件的负荷大于纯粹的邮件服务器，因此如果邮件安全产品和被保护邮件服务器使用相同配置的硬件，邮件服务器可能能比邮件安全产品承受更大的冲击。

9.3.5 保证自身安全

邮件安全产品是互联网与邮件服务器的必经之路，因此自身的安全尤为重要。如果邮件安全产品只考虑识别和过滤病毒邮件和垃圾邮件，而忽视了自身的系统安全，就有可能被入侵，而当邮件安全产品被入侵后，将导致邮件服务器所有邮件用户账号被曝光、邮件账号的相关口令被窃取、邮件被截取，这个损失将远远大于邮件服务器被垃圾邮件骚扰、甚至大于内部网络被病毒邮件感染的损失。

1. 关闭无用服务

邮件安全产品应提供尽量少的服务，将所有无用服务关闭。

2. 保护必需服务

SMTP 服务是必须的，因此要保证运行于 SMTP 协议的程序的绝对安全，发现任何安全漏洞需要在第一时间修补。

管理邮件安全产品的服务，可能是通过 https/ssh/串口等，除了应保证协议程序安全外，还应限制管理来源，例如不应该允许整个互联网通过 https/ssh 管理邮件安全产品，管理内部网络时可能需要绑定 MAC 地址等。

3. 建议用户使用加密协议

一般用户在使用邮件系统收发邮件时，使用 SMTP/POP3 协议，在使用 webmail 时，使用 HTTP 协议。应建议用户使用 SMTPS/POP3S/HTTPS 等加密协议，这样即使在邮件安全产品自身被入侵时，也不会使邮件口令被窃取。

4. 不要在服务器上保存邮件

所有邮件应及时下载到客户机上，而不是长时间、大量地保存在邮件服务器或邮件安全产品中，这样即使在被入侵时，也不会有太多邮件被窃取。

9.3.6 实时升级

实时升级是任何一个安全产品都应该具备的基本功能，反垃圾邮件系统也不例外。技术总是在不断地更新和发展，垃圾邮件的制造和伪装手段也是越来越高明，这也就需要不断改进和增强反垃圾邮件系统鉴别反垃圾邮件的能力。另外，反垃圾邮件系统自身也需要不断升级，以应对网络上的各种威胁。而系统中的病毒过滤模块更是需要及时更新才能够应对层出不穷的各种病毒。要达到这些目标，最好的手段当然就是通过网络实时升级。

实时升级需要系统在设计之初就考虑系统的可更新问题，系统应该尽可能地模块化，代码和数据应尽可能分离，以利于系统的更新和升级。另外，这也要求反垃圾邮件产品的制造商以服务的思想来看待反垃圾邮件产品，通过提供更好、更及时的升级服务来增强自己产品的反垃圾邮件能力和市场竞争力。

9.4 技术之美

技术之美，并非指的是一个产品包装有多么的漂亮、产品的外壳设计多好看，或者产品的界面如何花哨。

技术之美，指的是一项技术或产品的实现是美的，洋人有句话，叫做“Simple is the Best”可以说是对技术之美的精辟描述。一个产品可以称之为技术美的，必然是每一个实现的功能都采用了最简单、最直接、最清晰的方法，使用户在使用的时候，也许无需产品手册即可使之运行。

凭空说技术之美或“Simple is the Best”可能难以理解，或者太空泛，下面举一个例子。

以要求对邮件服务器进行全保护为例，所谓全保护，就是要求所有进出邮件都必须经过反垃圾邮件系统的保护，堵塞邮件服务器直接发出邮件的通道，并防止垃圾邮件发送者直接将邮件送入邮件服务器。

如果使用 MX 转发模式实现完全保护邮件服务器不被绕过，唯一的方法是：

- 用防火墙保证互联网无法直接访问被保护邮件服务器，在 DNS 的 MX 记录中也没有对被保护邮件服务器的指向设置。
- 为了使被保护邮件服务器在不被直接访问的情况下接收邮件，就必须对 HTTP/POP3/IMAP 等协议进行转发代理。

在 MX 转发模式下，实际的拓扑结构是“逻辑串连”，但在初步达到完全保护的同时（之所以说是初步，因为它要支持加密的邮件协议和其他协议需要单独编写许多代理程序），丧失了冗余的功能，也就是说这种模式下的 MX 转发模式产品如果发生故障，将同样导致邮件不能收发。

请注意：要实现这样的功能，还需要防火墙的协助，拓扑也不清晰优美。

因此，在只有一台运行反垃圾邮件产品的情况下，冗余和完全保护是互斥的，MX 转发模式也可以在防火墙的帮助下实现完全保护，但丧失了冗余。而透明模式完全保护邮件服务器无需防火墙协助，自己就可以完成。

也就是说，使用透明网关模式和使用 MX 转发模式实现邮件服务器的完全保护，其缺点是完全一样的，而透明网关模式自动支持 HTTPS/POP3S/IMAPS 等所有协议，比 MX 转发模式的产品强得多、直观得多。

注意：*不要以为网关模式增加了故障点，因此在产品的冗余性上就低于 MX 转发模式。MX 转发模式在一定的要求下，会丧失冗余。*

为了实现全保护，有些产品使用代理，但实际上，如果用户的防火墙支持针对端口的策略，则可能无需代理，因此这样的实现完全是画蛇添足。

使用 MX 转发加防火墙加代理的方法实现透明模式干净利落能实现的功能，存在透明模式同样的缺点，支持的协议还比透明模式少，这样比较起来，同样实现邮件服务器的全保护，透明网关模式的实现要优美得多。

9.5 性能测试

对反垃圾邮件系统进行性能测试也是一项非常重要的工作。通过性能测试，可以了解系统实际的工作效率和处理能力，评价系统方案的好坏，查找系统中可能存在的性能瓶颈，并据此对系统进行改进和优化。

由于反垃圾邮件产品是一个新产品，因此在测试方法上没有达到大家认可的统一，许多媒体、测试试验室及乙方的选型评测都很不完善，无法依据现有的测试方法得到可比较的判断依据。

9.5.1 测试条件

软件比较测试应该基于相同的硬件平台。产品比较测试可以基于实际产品，但应标注硬件平台特征。

9.5.2 对比测试

前面已经说过，反垃圾邮件产品存在各种各样的针对性技术，很难实现统一的测试方法，本章后面将说明每个技术方法的测试，但测试部门针对这些测试结果，必须给出相应的测试环境、针对的技术、样本针对性及测试方案，否则可能导致误解。

基于此，使用真实的网络环境和邮件环境，提供相同的测试环境进行对比测试，并给出总的结果和各种指标的结果，可以比较公平地测试现有的产品。

1. 测试目标

对比测试的测试目标可以如下设计：

- 一台或若干台邮件服务器；
- 被测邮件服务器应该具备根据特定的标志分离邮件的功能，可以分离出邮件是由哪台被测邮件安全系统发过来的；
- 被测邮件服务器应该具备以比较平均的方式将邮件转发给被测邮件安全系统的功能。

2. 测试环境

定义若干个被测邮件域，这些邮件域可能包括：

- 实际使用的、公开的邮件域；
- 不实际使用的、仅作为垃圾邮件测试的公开邮件域；
- 从未实际使用也从未公开过的邮件域。

这些邮件域的DNS服务器将对所有的被测邮件安全系统指定相同优先级的MX项，以保证所有邮件被公平地分发给所有被测邮件安全系统。

被测邮件安全系统对收到的邮件进行反病毒邮件、反垃圾邮件处理后，应标上相应的标记转发给邮件服务器并保存日志，使邮件服务器能够根据标记判别该邮件是由哪台邮件安全系统发出的。考虑可能有多台相同邮件安全系统存在，该标记应至少包括邮件安全系统的IP地址。

邮件客户端将外发邮件发给邮件服务器，由邮件服务器公平地转发给被测邮件安全系统，经被测邮件安全系统处理后发出并保存日志。

9.5.3 功能测试

产品具有透明网关(Bridge Mode)、MX转发和独立服务器三种模式，可以灵活使用甚至同时使用。本次测试只测试了透明网关模式。

产品拥有动态控制、病毒识别、垃圾识别、内容过滤4个主要功能引擎，以及邮件审计、智能交互、状态与日志、公安监管4个辅助引擎。在产品反垃圾邮件、反病毒邮件时，主要依靠各个引擎和子引擎的配合以达到性能和效果上的统一，因此在测试时，根据不同的环境需求进行不同的配置会得到不同的性能结果和效果结果，因此在试验环境测试后，还在实际环境进行了测试。

9.5.4 性能测试

在性能测试方面，经过对用户实际需要的分析，将重点放在考察受测设备对于邮件的处理能力上。不管是工作在转发模式还是透明模式，各种受测设备最终还是要在本地处理SMTP命令和维护邮件队列。因此使用Spirent公司最新的Avalanche 2500和Reflector 2500设备来模拟一定的流量压力，考察反垃圾邮件网关所支持的邮件处理能力等重要参数。

在性能测试中，所采用的拓扑结构为：以Avalanche 2500模拟客户端向反垃圾邮件网关发送邮件，然后由反垃圾邮件网关转投给由Reflector 2500模拟的邮件服务器。

通过Avalanche 2500，可以对模拟邮件的源发送IP地址、目的IP地址、发件人、收件人、邮件的长度等参数进行设置。测试时，采用了一个C类地址来模拟源发送IP地址，为了模拟真实的邮件环境，模拟的邮件中有25%的邮件大小为300KB，其余邮件的大小

是在 0.3～30KB 之间平均分布的(即每封邮件的平均大小为 15.15KB)。

具体测试过程分为 5 个阶段：第一阶段是准备阶段，Avalanche 2500 准备发送模拟邮件；第二阶段是预热阶段，Avalanche 2500 模拟的邮件发送人数从 0 缓慢升到 10；第三阶段是逐步加压阶段，分 10 个步，每个步增长 50 个用户；第四阶段是维持阶段，即保持有 510 个用户同时做发信请求；第五阶段是结束阶段，用户数逐步减少到 0。整个模拟发信过程时长为 220s。

通过 Reflector 2500，设置了接收邮件服务器的域名(ccwtest.com)、IP 地址和端口号。在 Avalanche 2500 发送测试邮件的同时，Reflector 2500 开始对从反垃圾邮件网关转发过来的邮件进行分析统计，直到反垃圾邮件网关结束整个投递过程时停止测试。

通过测试，可以得到反垃圾邮件网关每秒提供 SMTP 服务的能力——最大并发连接处理数，同时可以得到发送邮件的连接请求数、成功发送的邮件数、成功转发邮件的百分比及平均响应时间等重要参数。需要说明的是，这些参数是在反垃圾邮件网关没有开启任何过滤策略时的数据，它们在一定程度上反映了反垃圾邮件网关在极限工作时能达到的状态。为了保证测试的精确性，进行了 3 次测试，测试结果取平均值。

测试指标说明

- 发送邮件的连接请求数：指在测试过程中，Avalanche 2500 测试设备向反垃圾邮件网关发出的 SMTP 请求的总数，如果请求没有得到响应，测试设备不会发送邮件。
- 成功发送的邮件数：是模拟邮件服务器 Reflector 2500 成功接收到的、由反垃圾邮件网关转发过来的邮件数。
- 成功百分比：是指成功发送的邮件数与发送邮件的连接请求数的百分比。
- 最大并发连接处理数：是指整个测试过程中，反垃圾邮件网关成功接收邮件的瞬间最大值。对整个性能测试来说，最大并发连接处理数是最重要的指标之一，它反映了邮件系统瞬间提供服务的能力，其结果表示为每秒建立的连接数。
- 平均响应时间：是指从 Avalanche 2500 发送 SMTP 连接请求开始，到反垃圾邮件网关成功接收到邮件第一位数据时的时间间隔。

9.5.5 内容分析测试

在测试环境中，采用了自行研发的测试工具，结合 qmail 系统进行邮件的发送。虽然开发一个邮件发送程序非常简单，但单一的邮件发送模式无法模拟垃圾邮件多变的制造环境，而 qmail 是一种很常见的 MTA，使用 qmail 可以有效地确保邮件发送的兼容性和真实性。例如，所有垃圾邮件的邮件路由信息都被保留，其中往往包括了假的 IP 地址、主机名或 E-mail 地址信息。这些信息都可以成为受测设备判别垃圾邮件的条件。

所采用的拓扑结构为：通过一台配有 MTA(邮件传输代理)的发件服务器 A 向受测设备发送样本邮件，受测设备对邮件进行过滤处理后再发给收件服务器 B。在服务器 B 上建立了若干专用于接收邮件的邮件账号，每次测试完毕后对处理结果进行统计和分析。

在测试环境中建立了实验域 test.com，为测试环境中的主机建立相应的 A 记录，并将 MX 记录指向受测设备，然后设置受测设备将邮件转发到收件服务器 B。使用的样本邮件包括 62 335 封病毒邮件、62 335 封垃圾邮件和 500 封正常邮件。邮件样本的平均长度为 14KB，其中约 30％含有附件。500 封正常邮件，包括普通的工作往来信函、订阅的邮件列表和朋友间的群发邮件等。在测试中，还对上述样本进行了随机发送，即有些邮件可能被随机发送了若干次。

由于测试环境的所有邮件都是从 MTA-A 发出的，因此无法测试智能 RBL 和可追查性检查的效果，因此关闭了智能 RBL 和可追查性检查，可追查性检查的测试在后面的实际环境测试中测试。

开启贝叶斯过滤器(无预置学习库)、智能集中分析、分类内容过滤和降噪系统。由于对于未知的垃圾邮件，静态内容过滤没有意义，因此没有开启。

结果如下：

- 病毒邮件屏蔽率 100％。
- 垃圾邮件屏蔽率 100％。
- 垃圾邮件误报率 0％。

得到上述结果令人有些意外，经测试人员分析，认为通过垃圾邮件探针邮箱采集到的垃圾邮件应该是互联网上泛滥程度最大的邮件，在系统使用的 3 个智能集中分析服务器(DCC、Razor、Pyzor)中应该已将上述垃圾邮件置于很高的垃圾可能性，因此被全盘封锁。

9.5.6 性能比较和选择

目前许多产品以“多少多少用户数”来判断应该使用的产品的性能档次，这实际上很不完全，因为同样用户数的邮件服务器，由于其用户使用的频繁程度不同，因此应该考虑更多的数据：

- 邮件系统用户数；
- 每天邮件系统收邮件总数、发邮件总数(多少封)；
- 每天邮件系统收邮件总量、发邮件总量(多少 MB)；
- 邮件系统最大、平均并发 SMTP 连接数。

另外还要将产品在实际或模拟环境中实测以下内容：

- 病毒邮件爆发时，邮件安全产品为阻挡病毒邮件产生的负荷(每天阻挡多少病毒邮件增加了多少系统负荷)；

- 垃圾邮件爆发时，邮件安全产品为阻挡垃圾邮件产生的负荷（每天阻挡多少垃圾邮件增加了多少系统负荷）。

基于这些参数，参考实际系统的运行情况，并考虑一定的冗余（以备用户量增加、用户用量增加或病毒邮件、垃圾邮件爆发），就可以比较准确地确定邮件安全系统合适的配置。

根据经验，一般邮件服务提供商所使用的邮件服务器的平均负荷远远低于企业邮件服务器的平均负荷，这个原因很简单，企业邮件服务器处于局域网，因此一般使用频度（每人每天发送的邮件数）高、使用量（经常发送大邮件）大；而邮件服务提供商的用户使用远程连接来连接邮件服务器，一般不会发送大量、很大的邮件。