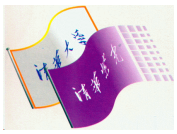
紫光安全
UnisGate



清华紫光UnisGate安全网关
反垃圾邮件管理手册

2005年3月

清华紫光股份有限公司
网络安全产品事业部

前言

目录

表格目录

图形目录

1 简介

1.1 技术说明

本产品支持目前所有的反垃圾邮件技术，并结合本公司专利技术，达到了性能与效果的完美统一。

本产品具有透明网关、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。

本产品拥有动态控制、病毒识别、垃圾识别、内容过滤四个主要功能引擎，以及邮件审计、智能交互、状态与日志、公安监管四个辅助引擎，能够完美、高效地控制本地发出病毒和垃圾、防止接收外来病毒和垃圾，是类似产品中最优秀的产品之一。

本系统的主要功能引擎的控制流程为：

1. 【动态引擎】－【同时连接数】：动态控制引擎的同时连接数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，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三个重复控制引擎限制同一发件人、同一主题、同一IP的邮件的发送频率，并可能阻挡未知病毒和垃圾的泛滥程度；

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、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】－【智能实时黑名单】：智能实时黑名单将这些黑名单列入的匹配邮件(注意：不仅是最早的RBL的IP列表)判断为垃圾邮件；

7. 【内容过滤引擎】：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智能内容分析来判断该邮件是否垃圾邮件，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。

1.2 设备安装

本设备为有三种模式，不同模式时使用不同的安装方法：

1. 透明网关：内口用交叉网线连接被保护的邮件服务器，外口连接互联网(一般是通过交换机接路由器)
2. MX转发：只使用外口，连接互联网。一般通过交换机接路由器，交换机上连接其他被保护的邮件服务器。
3. 独立服务器：只使用外口，连接互联网

注意： 三种模式在产品系统实现上是相同的，并且三种模式可以共存，即本设备可以放在被保护邮件服务器前，作为透明网关保护邮件服务器；同时可以将另一邮件服务器的MX最高优先级指向本设备管理IP，以MX转发模式保护这第二台邮件服务器，同时在本设备上还可以定义自己的邮件域。

本设备支持多机、多域，即被保护的任意邮件服务器可以有多个邮件域，同一台本设备可以保护多台邮件服务器。

内外口可以任意使用，如果按系统定义反方向使用本设备，只有在[日志监控]-[系统状态]的内、外网流量会出现相反的情况，其他完全一致。

有防火墙时防火墙的设置： 即使在透明网关模式，本设备也不是全透明的，对SMTP协议(25端口)是截收、转发的方式，并使用了互联网的一些服务，因此必须保证本设备的管理IP拥有必要的网络权限(比如防火墙策略、交换机路由器的ACL等)，在其他两种模式，当然更需要。包括：

内向外的smtp访问(目的端口=25)，允许网关将处理完的邮件转发出去。注意：在透明网关模式外到内不必设置(外到内应该已经为邮件服务器设置了)，因为外到内访问的是邮件服务器、被网关截收，因此不涉及网关的管理IP；

内向外的dns访问(目的端口＝53)，网关要转发邮件，必须使用dns服务得到目的方的IP；

智能分析服务器：双向的(本地IP=网关管理IP，远程IP=任意，本地端口=udp1023，远程端口=udp6277)访问；内到外的tcp 7和2703端口访问；内到外的tcp和udp的24441端口访问。

上述3项中，1、2是被保护服务器本应具有的网络权限，3是智能分析服务器需要的。

1.3 管理界面

AntiSpam系统为Web管理界面，使用IE等浏览器访问系统管理IP地址(http或https，建议使用https协议，除非网络速度很慢或系统负荷很重时)。

- 系统缺省管理IP：192.168.0.150。与以前的V1.x版本不同的时，V2.0的管理IP任何一个口都可以访问；
- 管理URL：https://192.168.0.150/admin/
- 用户Web客户端界面URL：https://192.168.0.150/ （独立服务器模式）

  注：部分产品应客户的要求，管理URL和用户Web客户端界面URL改为：
- 管理URL：https://192.168.0.150
- 用户Web客户端界面URL：https://192.168.0.150/mail/wmail （独立服务器模式）
- 缺省系统全权管理员用户名：admin，口令：admin。

系统左边为管理菜单项，从该树形菜单可找到所有管理页面，在页面中设置系统参数，系统参数为实时生效，即当一个页面的[确认]被点击时，对该页面的配置马上生效。

系统分三大部分：系统管理部分、防垃圾配置部分和日志分析部分。

系统管理部分包括：系统设置、管理员和三种运行模式：透明网关、MX转发和独立服务器。

防垃圾配置部分目前包括六大引擎：动态限制、病毒识别、垃圾邮件(合法性检查)、内容过滤、邮件审计和智能交互。

日志分析部分包括主菜单：日志监控和公安网络监管。

2 系统管理

2.1 序列号和许可证

本产品使用序列号标记每个产品，序列号和系统硬件相关。License是根据序列号，由厂家生成的License文件，因此也和硬件相关，即硬盘换到另一台硬件上系统无法使用。当License未安装或无效时，可将管理界面显示的序列号返回厂家，由厂家重新生成License文件导入。

正常产品应该在本页面有“本设备License许可正确”的提示。

2.2 升级更新

管理员可以从厂家网站、客服等处得到升级包，从本界面上载升级。系统会自动检测升级包和对应的版本，因此不符合要求的升级包系统不会升级，而是提示错误。如果同时得到几个升级包(可能针对不同的改进)，必须按升级包主文件名的最后两位的顺序逐个上载，否则小号码的升级包将无法再上载。

2.3 运行模式

本产品支持透明网关、MX转发、独立邮件服务器三种模式。确定的客户得到的可能是其中的一种模式。

透明网关：这种模式时本产品插入到被保护的邮件服务器前，内口可通过交叉线连接被保护的邮件服务器，外口连接原邮件服务器的接口(交换机或路由器的口)，这是本设备的角色是个网桥，原邮件服务器无需改动任何配置参数，只需配置本设备即可正常工作。透明网关模式的缺点是增加了故障点，当本设备出现问题时就无法收发邮件。

MX转发：这种模式时本产品和被保护邮件服务器都接入互联网中，用户域名的DNS服务器应该将最高优先级的MX项指向防垃圾邮件系统，其他邮件服务器出于较低的MX项。这样邮件首先被递送到本系统，本系统做完处理后，才将允许通过的邮件转发给其他邮件服务器。当本系统出现故障无法接收邮件时，发件方会自动寻找优先级次高的邮件服务器发送，这样回避了透明网关方式时的单点故障问题。但垃圾邮件发送者可以直接向被保护的邮件服务器发送，这样就躲过了垃圾邮件的检查。

独立服务器：这种模式适用于新建邮件系统或替换原来的邮件系统，无需另有邮件服务器，同时自带POP3服务器和Web邮件客户端。目前适用于中小型邮件服务器。

2.4 网络设置

主机名称：本设备的机器名(FQDN)，即hostname，最好对应域名，不

对应也无所谓

IP/网络掩码：本设备的IP和掩码，用于和互联网通信和管理。

网关：和被保护邮件服务器的出口网关相同。

上述三种运行模式下都需要配置这四个参数。

2.5 SMTP基本参数

SMTP的基本参数，一般可以使用缺省值。

服务器名：本机mail系统必须设置的一个名字，建议使用被保护邮件服务器的域名直接作为这个服务器名

SMTP HELO主机名：网关外发邮件时的时候，和别的smtp服务器打招呼时候的helo 后面跟的名字，需要设置为可以被解析的域名（建议设置为被保护服务器的名字），因为目前有些smtp服务器会判断这个helo 的名字，如果不可解析就会拒绝邮件；

SMTP问候语：其他SMTP服务器连接过来看到的第一行信息；

SMTP连接超时：建立网络连接的最长等待时间；

SMTP发送邮件超时：在将邮件投递给其他邮件服务器时，SMTP协议交互每一行命令的最长等待时间；

SMTP接收邮件超时：在接收其他邮件服务器投递过来的邮件时，SMTP协议交互每一行命令的最长等待时间；

最大邮件尺寸：允许发送邮件的最大尺寸；

邮件队列投递超时：如果收件方由于网络不通等临时故障而无法将邮件投递出去，放弃投递邮件之前的最长等待时间；

本地并发投递数：最大的本地（独立服务器模式下）的投递并发数；

远程并发投递数：最大的远程投递并发数，远程投递是指由网关发给外界的动作；

2.6 配置管理

配置管理可以将本设备的配置文件和内容过滤策略文件分别下载保存，也可以将保存的文件上载到系统中。

2.7 系统时钟

系统时钟应该准确，以保证邮件、日志的时间准确易于查找。在本页面中可以对AntiSpam网关的时间进行设置：

可以在输入框写入时间，然后提交，本设备时间就更新为输入框的时间定义；

可以选中[同步本地]，这样本地时钟就自动显示在输入框中，并每秒更新，点击[提交]，本设备时间就更新为当时输入框的时间。

2.8 系统重启关机

由于设备文件系统可能有未存盘内容，因此请使用本页面的软开关来关机或重启。

但本设备在文件系统上做了保护，一般意外的断电不会导致系统损坏，但是有可能导致信件丢失。

2.9 退出系统

退出本Web管理界面。为了防止有人有意或无意使用本管理界面非法管理本系统，管理员离开管理用机时，应该退出管理界面。

3 管理员

3.1 管理员管理

系统可以有多个管理员。在这里增加、删除其他管理员，或帮助其他管理员修改口令。

注意：无法得到其他管理员的口令，当其他管理员忘记口令需要你帮助时，只能帮他修改口令。

注意：管理员无法修改自己的除口令和可登录管理的IP列表以外的任何属性，只能修改别的管理员的属性，这是为了保证权限的相互控制。

管理员相关属性包括：

1. 帐号名/口令：该管理员以此帐户名和口令登录本系统进行维护工作。
2. 管理权限：该管理员所拥有的权限：
   (a) 管理员：
   (b) 系统管理：
   (c) 动态限制引擎：
   (d) 垃圾邮件引擎：
   (e) 病毒识别引擎：
   (f) 内容过滤引擎：
   (g) 智能交互引擎：
   (h) 邮件审计引擎：
   (i) 日志监控：
   (j) 操作日志管理：

(k) 独立服务器管理：独立服务器模式的管理

(l) 网关中继管理：透明网关模式和MX转发模式的管理

(m) 公安网络监管：

3. 只读：该管理员只能查看系统配置情况，不能修改。

4. 禁止登录：可以临时禁止某个管理员登录，这样不想让该管理员登录时不必删除该管理员

5. 备注：

6. IP限制：为了保证管理安全，[允许]或[禁止]该管理员从这里列出的IP范围登录，也可以选择[不限制]，则允许该管理员从任何IP登录管理。

7. 管理邮件域：该管理员可以管理的本地域(独立服务器模式)

3.2 登录限制

为了防止有人试探管理员口令，可设置登录限制。
注意：设置后封禁的是该登录机器的IP而不是该用户。

3.3 修改口令

修改别人的口令在[管理员列表]中针对该管理员操作。这里是目前登录的管理员修改自己的口令。

注意：这应该是设备开始使用的第一件事：将系统的缺省管理员Admin的口令改为自己的口令。

3.4 修改IP限制列表

管理员可以控制自己从何处(IP范围)登录或禁止从何处以自己的名义登录。

在文本框中输入“IP/Mask”，每行一个，然后选择允许还是禁止，或者不限制。

4 透明网关模式

4.1 邮件域保护设定

本系统在透明网关模式支持多机多域，即被保护的邮件服务器可以接收多个域名的邮件，例如虚拟邮件服务器的情况，同时一台本系统可保护

多台邮件服务器。被保护的邮件服务器可接收的所有域名需要在这里定义上。

邮件域：被保护的邮件服务器可以接收的邮件的域名

IP地址：被保护的邮件服务器的IP地址

端口：被保护的邮件服务器可不使用缺省的25端口，本系统外口接收25端口的smtp请求，因此内部邮件服务器使用任何端口都可以，只要防垃圾网关和被保护邮件服务器配置相同即可。

备注：

4.2 邮件队列监管

当前系统邮件队列中正在收发的邮件，可以批量删除或清空。

注：

在队列监管中，总发现一些邮件停留在队列中，原因是这样：系统设置了垃圾邮件为[标记后转发]，或是因为某些原因漏判进来的垃圾邮件，这些邮件的目的地址在服务器上并不存在，因此邮件服务器产生退信，而如果这些邮件的发件人地址又是伪造的，会导致退信无法发出，因此滞留在队列中，直到超时(正常可发出的邮件在队列中存在的时间很短)。

退信很明显：没有发件人地址。这些退信可以在邮件队列监管管理界面上删除。

产生这种不可达退信的原因是对不可追查的邮件做了“标记后转发”而不是“拒绝”，因为目前网关无法判断收件人是否确实在被保护服务器上存在。如果使用某种方式，例如如果被保护邮件域有ldap服务，网关可以利用ldap服务来判断收件人是否确实存在，就可以防止这种情况发生。我们也在考虑采用其他方法解决这个问题，因为使用ldap服务的邮件服务器很少。

5 MX转发模式

MX转发模式主要是网络拓扑与透明网关模式不同，这些不同处于系统内部，因此其设定与透明网关模式相同，也因此邮件域保护和邮件队列监管这两个页面和透明网关是完全相同的，无论在哪里设定，在另一个地方同样。

5.1 邮件域保护设定

本系统在MX转发模式支持多机多域，即被保护的邮件服务器可以接收多个域名的邮件，例如虚拟邮件服务器的情况，同时一台本系统可保护多台邮件服务器。被保护的邮件服务器可接收的所有域名需要在这里定义上。

邮件域：被保护的邮件服务器可以接收的邮件的域名

IP地址：被保护的邮件服务器的IP地址

端口：被保护的邮件服务器可不使用缺省的25端口，只要本系统和被保护邮件服务器配置相同即可。但非25端口的邮件服务器不能直接从外部邮件服务器接收邮件，丧失了在本系统失效时仍然能接收邮件的优点。

备注：

5.2 邮件队列监管

当前系统邮件队列中正在收发的邮件，可以批量删除或清空。

6 独立服务器模式

6.1 独立服务器设置

本系统可以作为独立的、具有防垃圾邮件功能的邮件服务器使用，在独立服务器模式需要定义本系统(即本邮件服务器)允许接收的域，这里也支持多域。每个域需要定义如下信息：

- 邮件域：独立服务器模式时允许接收的域，就是邮件地址@后的部分。
- 管理员：哪个管理员可管理这个邮件域
- 用户限额：本邮件域每个用户的空间限制
- 空间限额：本邮件域的总空间限制
- 备注：

6.2 邮件队列监管

当前系统邮件队列中正在收发的邮件，可以批量删除或清空。

注意：三种模式的邮件队列监管是完全相同的队列，因此在哪个模式的这个菜单看到的都是相同的内容。

6.3 本地用户管理

独立邮件服务器模式时，需要在这里维护本地邮件用户信息。

6.3.1 用户管理

在[管理员]-[管理员管理]或[独立服务器模式]-[独立服务器设置]中，我们已经设定了每个管理员可管理的本地邮件域。在本菜单项中，首先选择邮件域当前管理员可管理的本地邮件域之一，然后维护该邮件域用户的信息。

6.3.2 查找用户

首先选择邮件域当前管理员可管理的本地邮件域之一，可查找该域的用户，查看其的详细信息。

查找用户必须输入准确的用户名。

6.3.3 用户组管理

可建立用户组的名字，每个用户属于哪个组在[用户管理]中设置。设置用户组的目的是为了管理员管理需要，从本系统管理界面群发邮件。

6.3.4 群发邮件

在这里，可以向上面定义的用户组群发邮件。

7 动态限制引擎

动态限制引擎可以将垃圾邮件发送速度大大降低，同时基本不影响正常邮件的收发。

在每个动态限制引擎中，可以定义白名单，白名单中的对象不受该动态限制限制。

注意：这里的白名单与[垃圾邮件引擎]-[垃圾识别]中的白名单不是一回事。

7.1 基本设置

基本设置包括单选的引擎开关和多选的作用方向。

由外向内的作用方向：是被保护的邮件服务器在接收其他邮件服务器发来的邮件时的情况；

由内向外的作用方向：是被保护的邮件服务器在发送邮件到其他邮件服务器时的情况。

7.2 同时连接数

同时连接数，是单个IP的并发连接数，为了区分通常定义的并发连接数如此命名。也就是单台外部邮件服务器或计算机(单个IP)可以同时与本系统建立的smtp连接数。

管理员可根据情况设置，设为0表示不限制。

注意：并发连接设置无论保护方向设置为任何值，都保护且只保护‘外到内’的方向。

在同时连接数控制中，可以设置IP白名单，在该名单中的IP将不受同时连接数限制。

同时连接数的控制对自动发送的垃圾邮件非常有效，可以大大降低垃圾邮件的发送速度。同时，对正常邮件影响不大，因为正常的对方系统会自动重试发送。

7.3 连接频率

同一台机器(同一IP)在设定时间中最多可发送的邮件数。如果超过此限制，每试图多发送一封，将封禁他设定的时间。该封禁时间会根据超限的封数累积，同时根据时间的流逝减少。

连接频率和同时连接数的区别是：同时连接数是单个IP可以与本系统并发的smtp数，而连接频率是在定义的时间内只允许定义次数的smtp连接发生，一旦超限就根据定义封禁，而此时的并发连接可以是1，但一个个连接建立和完成的时间很快。

连接频率尤其对内部用户外发垃圾或病毒邮件有很强的抑制作用。

7.4 用户重复限制

同一发件人在设定时间中最多可发送的邮件数。如果超过此限制，每试图多发送一封，将封禁他设定的时间。该封禁时间会根据超限的封数累积，同时根据时间的流逝减少。

在用户重复限制种，可以设置用户白名单，在该名单中的发件人将不受用户重复数的限制。设置用户白名单有可能导致垃圾邮件发送人知道该名单中的人后使用这些用户名发送，但实际情况是很少发生的。

这种动态封禁对大量发送的垃圾邮件非常有效，自动发送垃圾邮件的机器如果使用同一发件人，常常被封禁数小时甚至数天，这样实际系统只放过了很少的垃圾邮件。

7.5 邮件重复限制

邮件重复限制和用户重复限制类似，只不过用户重复的判别标准是发件人，而邮件重复的判别标准是主题。

其白名单及副作用、有效性都和用户重复限制类似。

7.6 实时管理

上述类似的3种重复限制将导致超限封禁。系统管理员可以经常观察[实时管理]中这三种限制的实时情况，可以发现谁正在大规模发送垃圾邮件、是否有正常邮件但超限了而被封禁，这时管理员可以手工解除封禁。

注意：实时管理中所列出的“重复数据”不是总共重复了多少次，而是最近的、系统定义的时间内重复了多少次。

8 病毒识别引擎

病毒识别引擎是检查邮件是否被病毒感染。病毒库每2小时自动更新。

8.1 基本设置

这是病毒检查的总开关，可以指定检查接收邮件还是检查发送的邮件。

8.2 病毒识别

病毒的抽样检查。本引擎可以不100%检查邮件是否有病毒，比如平时可以只抽查50%，当发现病毒后在100%检查。

这在病毒不泛滥时，可以提高系统性能。

8.3 病毒处理

8.3.1 转发设置

对于上述病毒的检查结果，可以将该邮件：

- 标记后通过：可以按下面的文字标记邮件有，允许通过的将经过以后的系统处理
- 永久弹回：发件机器的SMTP握手将收到错误信息，如果是邮件服务器，会返回发件人带有被拒绝理由的邮件。系统负荷低。
- 直接丢弃：发件方不知情的情况下丢弃，系统负荷最低。

8.3.2 标记参数

对于上述病毒检查的结果，可以在邮件头(一般用户看不见，在邮件源码中)和主题上标记，同时，可以在邮件头中标记原因。

在主题上标记的文字可以自行设定，要求便于用户客户端自动分类。

9 垃圾邮件引擎

垃圾邮件引擎是检查邮件的合法性，又称合法性检查。

垃圾邮件识别分三大类：黑白名单、可追查性检查和智能检测，这三种方式保证了垃圾邮件识别的效果和性能。

9.1 基本设置

这是合法性检查的总开关，每种合法性检查都可以单独开关。

9.2 黑白名单

可设置针对IP(发送邮件的机器的IP)、邮件域名(发件人的域名)和邮件帐号(发件人邮件地址)的黑名单和白名单。

黑名单中的项目认为是已知的垃圾邮件发送者，不做可追查性检查，打上【黑名单】标记直接进入下一阶段的内容过滤（或直接丢弃）。

白名单中的项目认为是已知的非垃圾邮件发送者，不做可追查性检查直接进入下一阶段的内容过滤。

每个黑白名单均可单独打开或关闭。

9.3 可追查性检查

基于专利技术的可追查检查是本系统高性能、高准确性的中心，它根据互联网上可得到的信息分析发件人、发件邮件服务器是否是合法的、是否可追查得到发送此邮件的人或机器来判别。凡是可追查得到的，就通过可追查性检查，凡是追查不到的，就无法通过可追查性检查。

由于互联网上不存在这样的准确的数据，因此只能通过可得到的数据进行分析和估算。

在配置页面中，建议用户按“邮件”、“IP”、“域名”的顺序打开检查，建议全部打开。

同时可以调节2个宽限标准，认为是“垃圾邮件”或“疑似垃圾”的可分别调整其宽限程度。这两个宽限刻度建议使用缺省值。

由于存在宽限标准，因此有漏判的可能，但实践证明低于3%。

可追查检查有一定的误判可能，但实践证明低于1%，同时我们的系统具有专用的可追查性检查补偿网站降低误判率。建议用户将误判的邮件的邮件头转发客服，这样我们可以逐渐降低误判。

注意：由于可追查性检查需要在互联网和厂商的服务网站上取得数据，因此该特性无法在测试环境中测试，但在实际效果中，它具有极高的效果和性能的统一。

9.4 智能检测

智能检测全部是基于内容分析或投诉机制，是根据内容确定邮件是否垃圾的算法。

9.4.1 贝叶斯过滤器

贝叶斯过滤器是根据贝叶斯准则和贝叶斯定理，以已知垃圾邮件和非垃圾邮件为样本、来判断下一封邮件是垃圾邮件的概率。

因此贝叶斯过滤器需要已知的邮件作为样本进行自学习。

本系统的所有引擎和子引擎是互动的，即包括可追查检查、智能实时黑名单、智能集中分析和智能内容分析得出的垃圾邮件和非垃圾邮件都会作为贝叶斯自学习的样本，同时贝叶斯过滤器认为是垃圾邮件的邮件会作为智能集中分析等子引擎的提交邮件，充实智能集中分析系统的特征库。

9.4.2 智能实时黑名单

实时黑名单(RBL，Realtime Blockhole List)，是最早的防垃圾邮件技术，主要用于屏蔽OpenRelay和鼓励转发垃圾邮件的服务器。

至今，类似技术已经衍生了很多增强和扩展的黑名单服务，本设备中内置了国际最著名的11种改进的实时黑名单服务，可保证垃圾根源被预防相对彻底。

9.4.3 智能集中分析

智能集中分析是将认为是垃圾的邮件提交给分析服务器，由分析服务器提取特征，同时根据提交总数量、频率等参数认定它是垃圾邮件的可能性。这样的系统可以集合全球的邮件特征，将大范围发送、但局部数量并不多的垃圾邮件甄别出来。所有支持智能集中分析的防垃圾邮件系统都回互相促进、提高准确性。

9.4.4 智能内容分析

智能内容分析是根据目前垃圾邮件的主要内容特征认定其是垃圾的可能性。

9.4.5 智能降噪系统

智能降噪系统是指例如一个合法邮件发送者平时都是发送正常邮件、突然大量发送垃圾邮件时的情况，有可能是因为某种原因的错误判断，也就是可能是噪声，因此对其进行降噪处理，认为他发送的邮件是垃圾的概率相对降低。

9.5 垃圾处理

9.5.1 转发设置

对于上述合法性的检查结果，可以将该邮件：

标记后通过：可以按下面的文字标记邮件，允许通过的将经过以后的系统处理

永久弹回：发件机器的SMTP握手将收到错误信息，如果是邮件服务器，会返回发件人带有被拒绝理由的邮件。系统负荷低。

直接丢弃：发件方不知情的情况下丢弃，系统负荷最低。

9.5.2 标记参数

对于上述合法性检查的结果，可以在邮件头(一般用户看不见，在邮件源码中)和主题上标记，同时，可以在不可见的邮件头中标记原因。

在主题上标记的文字可以自行设定，要求便于用户客户端自动分类。

匹配黑名单的会被标记上【黑名单】。

10 内容过滤引擎

10.1 基本设置

引擎开关和过滤方向。

10.2 规则管理

在这里增加/删除内容过滤的规则

10.3 类别管理

上述规则可以分入本页面定义的类别中。

10.4 列印规则

当前规则总览，页面可以打印。

10.5 自定义文件类型

这里定义的文件类型将用于[规则管理]的规则中有关附件的内容。

11 邮件审计引擎

邮件审计引擎主要用于内部邮件审计和病毒、垃圾邮件分析。

出于对隐私权的考虑，目前不提供任何人查看被审计引擎保存的内容的查看，只能通过“公安监管”的“四部委交换格式”导出给公安部门查看。

11.1 基本设置

引擎的开关。

11.2 选择归档

归档的选择包括：

全部或部分归档；

部分归档可根据垃圾邮件、病毒邮件、动态超限邮件和匹配规则邮件四种类型归档，分别对应垃圾邮件引擎(合法性检查)、病毒识别引擎、动态限制引擎和内容过滤引擎的处理结果。注意：选择审计的选项两两内部是或的关系，四组间是与的关系，这样的逻辑关系稍显复杂，但可以满足很多需求。

同时，可将归档的邮件发往特定的邮件地址。

12 智能交互引擎

智能交互引擎是为了使本系统与发件人交互，让发件人知道本系统对邮件大小、发送重复等方面的限制，使合法的发件人能够在合法邮件被控制时，适当调整邮件发送习惯，保证邮件的发送。

智能交互引擎主要针对一些习惯不良的邮件使用者，比如以内部网邮件的方式使用互联网邮件，全不顾及别人的接收带宽等。

12.1 基本设置

引擎开关。

12.2 超大邮件提醒

系统对邮件大小有限制，同时对于习惯发送巨大邮件的发件人，智能交互引擎在允许他发送的同时提醒他邮件太大，以改变这些用户的发送习惯。

12.3 过量邮件提醒

系统的重复控制会对同一发件人短时间发送大量邮件或同一主题发送很多次数做限制，但这可能会影响合法的、大量接收人的邮件的发送，因此对这种情况，系统将做提醒。

12.4 病毒邮件提醒

由于目前许多病毒伪造来源，因此病毒邮件提醒应慎重使用，一般不用。

13 日志监控

13.1 系统状态

内网流量：被保护的邮件服务器和本设备内口间的相互流量

外网流量：本设备外口和互联网之间的相互流量，一般大于内网流量。

TCP连接：当时的TCP并发连接数。

SMTP连接：当时的SMTP并发连接数。

CPU负载：监控CPU负载是管理员日常工作，当CPU负载从远小于100%突然增大到100%时，应该注意观察病毒和垃圾邮件的情况，通常可能有病毒爆发。

内存使用：

硬盘负载：

硬盘空间：没有本地邮件用户和邮件审计时，硬盘空间应该占用很少，只是日志。如果硬盘空间有异常增加，应检查邮件对了监管，看是否有大量的邮件无法转发驻留在队列中。

13.2 引擎运行状态

邮件类别分布：病毒、垃圾等邮件在总邮件数中所占比例。正轴表示所有邮件，负轴表示正常邮件

邮件尺寸分布：各种大小的邮件所占比例

邮件流量分布：任何时间的邮件流量。正轴表示所有邮件，负轴表示正常邮件

DNS运行状态：由于收发邮件对DNS依赖很重，因此要监控DNS运行情况。正轴表示成功的请求，负轴表示失败的请求。

引擎运行状态：本设备各引擎运行时间和总时间。正轴表示实际时间(包含操作系统分时的等待时间)，负轴表示运行时间(不计算分时的等待)

13.3 日志显示

可显示当前日志内容。

可选中“实时监控”观察日志最新内容，可以比较容易地发现垃圾邮件、病毒邮件的泛滥情况。

13.4 日志统计

可做简单的统计：

一段时间范围内的：

总邮件数、垃圾邮件数、疑似垃圾邮件数

发件人地址、发件机器IP和匹配规则的Top10

更复杂的统计和分析应导出日志用其他工具来分析。

13.5 日志导出统计

由于统计会增大系统负荷，尤其在日志很大时，因此大范围的、更复杂的统计应该将日志导出，使用Excel、Access等软件做统计。

13.6 日志清空删除

日志应该在导出后清空，以免重复导致统计错误。

13.7 操作日志审计

保存管理员登录、退出及所做的操作。

14 公安网络监管

2004年2月初公安部、教育部、信息产业部、国务院新闻办等部门发文开始对垃圾邮件、病毒邮件和其他有害信息做专项整治，同时对有害信息要进行监管，各省市在四部委交换格式等统一要求下，做了监管的增强协议，各省市协议各不相同，因此需要对不同的协议使用不同的软件库完成，在本设置中用户需要根据他所在地区的监管协议进行选择。

14.1 基本设置

可以设置系统启用特定的一种网络监管协议，以此来和网络监管部门的系统通讯；

14.2 MSP设置

配置系统使用MSP1.8协议，适用于北京等地。

14.3 GAISC设置

配置系统使用GAISC协议，适用于辽宁等地。

14.4 四部委交换格式

按照四部委的垃圾邮件交换格式，导出当前所有被审计引擎记录的邮件。

注意：导出前应将邮件审计引擎停止，否则归档内容可能越来越大，如果网络速度不够快，可能永远导出不完。(V2.0正式版将自动完成此要求)

15 内部功能

为了使用户更清晰，本章说明一些内部实现情况，防止理解错误导致使用错误。

15.1 smtp认证

本系统提供了25端口的smtp/smtps认证的功能，无论原来邮件服务器是否必须使用smtp/smtps认证(即是否关闭了OpenRelay)，对于外发邮件，本系统将向被保护的邮件服务器转发smtp/smtps认证，如果认证通过且邮件的目的地址不在被保护的邮件服务器上，本系统将直接将邮件发出，而不转发给被保护的邮件服务器。

15.2 非完全透明

透明网关模式时，本设备的角色是一个网桥，因此两个网口可以任意使用哪个连接被保护邮件服务器，另一个连接网络。

管理IP是网桥的IP，因此从任何一个网口都可以连通。所有非SMTP协议(25端口)都被网桥直接转发，25端口被本设备截收，经过了防垃圾处理后，以管理IP的为发送源IP发出。因此管理IP必须有被保护邮件服务器IP完全相同的网络权限，包括防火墙策略、路由器交换机ACL等。

透明网关和MX转发模式时：对被保护邮件服务器，以及其他接收邮件服务器来说，管理IP是发送邮件的源IP；

透明网关模式时：对外面的发送邮件服务器来说，被保护邮件服务器IP是接收邮件的目的IP；

MX转发模式时：对外面的发送邮件服务器来说，本设备管理IP是接收邮件的目的IP；

15.3 高性能和降成本

由于本设备使用其他产品有用到的高负荷智能算法之前，先使用了低负荷、高性能的算法阻挡了95%的非正常邮件，因此相当于整体性能提高20倍。

同时，由于被保护邮件服务器无需承担这95%的非正常邮件，因此安装本设备后大大降低了被保护邮件服务器的性能需求，反之可以认为提高了被保护邮件服务器的服务能力。

16 FAQ

奇怪：接收邮件正常，本地用户用MUA发外地用户正常，Web用户发邮件都正常，只有本地用户用MUA发本地用户发不出，收到退信。

接收MTA要求所有Mail From是本地用户的都做认证，无论目的地址是本地还是远程，而邮件服务器的收发都经过了反垃圾网关转发，因此不可能认证。将邮件服务器设置：网关发的邮件无需认证即可。