

2007

瑞雷森科技（北京）有限公司

Dr.SMTP 业务部

[DR.SMTP 服务白皮书]



目录

- 1 Dr.SMTP 是什么? 2
- 2 Dr.SMTP 的面向客户群 2
- 3 Dr.SMTP 的服务 2
 - 3.1 DSN : Dr.SMTP Notify 黑名单预警及提示服务 3
 - 3.2 DSM : Dr.SMTP Monitor 邮件服务器的通信质量监测 3
 - 3.3 DSR : Dr.SMTP Relay 电子邮件全球无障碍收发 4
 - 3.4 DSCA : Dr.SMTP Certificate Authority 邮件服务器的审计与认证 5
 - 3.5 DSL : Dr.SMTP Frequency Limit List 垃圾邮件高频率控制列表 7
 - 3.6 DSC : Dr.SMTP Consultation 邮件/反垃圾邮件技术咨询 7

1 Dr.SMTP 是什么？

Dr.SMTP 是一个用于保障电子邮件服务正常运行的服务。

鉴于目前垃圾邮件泛滥，商业的邮件服务器都已经具备了相当程度的反垃圾邮件功能。而目前反垃圾邮件技术并未达到完全成熟，在消除了大量的垃圾邮件的情况下，还会带来一些邮件投递失败的副作用。在这种情况下，有的公司放弃了所有的反垃圾邮件措施，来保障其能收到任何投递来的信件（虽然绝大多数是垃圾邮件），但是也不能保障其投递出去的信件能顺利递交到收信人。因此，因噎废食的取消反垃圾邮件并不能根本的解决这个问题。

这种邮件投递失败不仅仅体现在邮件不能递交到收信人而退信，而且有时会发生邮件投递后被视作垃圾邮件而无任何反馈的直接丢弃，或者邮件尝试投递很长时间（有时长达几天）后才反馈消息说投递失败。后两种情况甚至比第一种情况还有糟糕，**邮件投递失败也许会给客户的商务活动造成不可估量的损失。**

在这种形势下，我们联合了中国反垃圾邮件联盟（CASA）及一些国际反垃圾邮件组织推出了 Dr.SMTP 服务来**诊断、救护和保障客户的合理的商业性邮件的安全可靠的投递。** Dr.SMTP 就像邮件服务的私人医生一样，为邮件服务的“健康”保驾护航。

2 Dr.SMTP 的面向客户群

Dr.SMTP 面向以电子邮件作为主要商务联络和以电子邮件作为主要业务的公司，包括：

- 外企办事处、外贸公司等经常和国外进行联络的公司
- 面向全国开展业务，拥有较多分支/办事处的公司
- 经营许可邮件列表发送的公司
- 经营商业电子邮箱服务的公司
- 以电子邮件作为重要商务沟通渠道的公司

使用 Dr.SMTP 需要您具备：

- 通过 IDC 托管的自行管理的电子邮件服务器
- 通过电信/网通等 ISP 的专线连接的自行管理的电子邮件服务器

3 Dr.SMTP 的服务

Dr.SMTP 所提供的服务有：

3.1 DSN : Dr.SMTP Notify

黑名单预警及提示服务

无论是无意间还是被恶意利用的发送了垃圾邮件，您的服务器 IP 地址都会很快被各大垃圾邮件组织捕获到，并列入其维护的实时黑名单中。被列入黑名单，惯例上是不会通知 IP 的使用者或所有者的（当然其中也有技术原因）。实时黑名单作为使用最普遍，同时也是认可度较高的一种反垃圾邮件手段，被很多邮件服务器所使用。

被列入黑名单后，使用黑名单的邮件服务器通常会无条件的拒收来自您的邮件服务器的电子邮件。

针对这种情况，我们推出了黑名单的预警及提示服务，可以对您的服务器的 IP 地址进行实时监测，如果一旦被列入了黑名单，我们会通过各种方式通知您，并协助您处理。

我们与 CASA 建立的合作关系，可以让我们随时监控到 CASA 的实时黑名单情况，在您的 IP 地址被捕获到（认定的）垃圾邮件后，即将加入黑名单前，提供一个迟滞期。在迟滞期间，我们会协助您处理您邮件服务器上垃圾邮件的相关情况，如果在迟滞期间能够解决该问题，并杜绝该问题的再次出现，则您的 IP 地址可以保障不被列入 CASA 的黑名单中。

同时，我们也会监控全球近百家具有影响力的、合理的、维护中的实时黑名单¹，如果您的服务器的 IP 地址被列入了他们的黑名单中，我们会通过各种方式，在第一时间通知您，并协助您脱离黑名单并解决您的服务器上可能存在的垃圾邮件问题。

之所以我们只能协助您脱离黑名单，是因为通常脱离黑名单，不仅仅是一个手续问题，而还需要对您的邮件服务器的状况进行了解，甚至获得服务器的管理权限，并且通常要求能以 IP 所有者或邮件域管理员的身份进行脱离申请。

3.2 DSM : Dr.SMTP Monitor

邮件服务器的通信质量监测

作为商业邮件服务器，保障其邮件通讯畅通是其重要的目标之一。作为邮件服务器的运营者，需要随时知道邮件服务器的运营状况，而这种持续性、长久性的监控要花费很多的时间精力和专业的技术力量。我们推出的邮件服务器的运营状况监测技术，就像为邮件服务器聘请的私人医生一样，可以及时跟踪邮件服务器的状况，并在发现异常时，将其通知运营者或解决该异常。

对邮件服务器的监测分为两个层次：

- I 级

通过邮件服务器上的监测账号与 Dr.SMTP 监控网格（DSG）之间的通信来监测邮件服务器的收信/发信是否正常。DSG 是 Dr.SMTP 建立的用于监控邮件互通的网格，包括国内外各大邮件服务提供商及多个客户之间的邮件交换，通过它可以实时判断邮件互通问题。

¹ “具有影响力”指其被广泛使用；“合理”是指其不会武断加入整个国家/地域的全部 IP 地址，而是根据实际情况确定是否加入黑名单；“维护中”指其还在继续维护数据，接受黑名单申诉。

除了按月提交监测报告外，在遇到邮件互通问题后，我们会及时通过各种方式通知用户，并可协助用户解决。

使用本监测，需要在被监测的邮件服务器上设立监测邮件账户，该账户仅用于与DSG进行通讯测试。

- II 级

通过接收的服务器上邮件日志的监测和分析报告，真实体现邮件服务器的运营状况。日志的传递有多种方式，如 SYSLOG 方式、RSYNC 方式、FTP 方式等等。接收到日志后，通过日志分析报表系统，会生成分析报告，并提交给邮件运营者。

在监控到服务器的重大异常状况时（如邮件量急剧增长或减低、大量的蠕虫病毒邮件、大量的邮件投递失败等），我们会及时通过各种方式通知用户，并可协助用户解决该问题。

使用本监测，需要将被监测的邮件服务器的日志通过某种方式传输到 Dr.SMTP。

不同的监测级别对邮件服务器的通信监测的灵敏度和全面性有不同的差异。

下表列出了不同监测层次间的异同：

监测条件	监测内容	II 级	I 级
需要增加监测邮件账户	通过邮件服务器上的监测账号与 DSG 之间的通信来监测邮件服务器的通信是否正常	✓	✓
需要获取服务器的邮件日志	通过接收的服务器上邮件日志的监测和分析报告，真实体现邮件服务器的运营状况	✓	

3.3 DSR : Dr.SMTP Relay

电子邮件全球无障碍收发

如果您的邮件服务器由于一些原因较长时间内不能与收件服务器通信，如：

- 邮件服务器的 IP 地址被永久列入一些黑名单中（如一些国外的黑名单将整个中国的 IP 地址都列入了黑名单）
- 服务器的通信模式不被收件服务器所接纳（如没有正确配置的 HELO/EHLO）
- 服务器 IP 地址没有反向解析
- 脱离黑名单需要较长的处理时间

为了避免邮件服务的中断，我们可以提供 Dr.SMTP 转发网络（DSR）来临时性为您转发邮件。通过我们的 DSR，可以让您的邮件透明的忽视这些问题，直接投递到您的客户手中。

3.4 DSCA : Dr.SMTP Certificate Authority

邮件服务器的审计与认证

通过对邮件服务器的审计,可以让您对您的邮件服务器的安全状况有一个全面而专业的了解。

审计之后会出具审计报告。审计内容包括两大方面:

- 邮件服务器的安全性

邮件服务器如果存在安全性问题,会被利用发送大量垃圾邮件。发送垃圾邮件的结果是一方面浪费了大量的服务器带宽和 CPU 处理能力;另外一方面服务器的地址和域名会被加入黑名单中,从而造成整个邮件服务器的邮件投递困难。

- 邮件账户安全

- ◆ 弱口令账户

如果邮件服务器上存在弱口令账户——如口令和用户名一样、口令过于简单(数字、英文单字等)、口令过于短等——这种邮件账户有很大的可能被垃圾邮件发送者扫描到,并利用这些账户发送大量的垃圾邮件。

- 滥用防护

如果邮件服务器由于配置漏洞,导致邮件服务器存在开放转发(Open Relay)或开放代理(Open Proxy),那么这些漏洞会被垃圾邮件发送者利用来发送大量的垃圾邮件。

- ◆ 开放转发

如果邮件服务器的发信不需要认证,那么任何人都可以通过该邮件服务器发送(垃圾)邮件。通常经过正确配置的邮件服务器都会对邮件发送进行限制或认证。

- ◆ 开放代理

开放代理是服务器上存在无限制的代理服务(Proxy),垃圾邮件发送者可以通过该代理服务连接到其它邮件服务器而递交垃圾邮件。这种开放代理通常出现在配置错误的 Squid 服务器或未限制的 Apache 的 mod_proxy 模块。

- 发送检查

如果邮件服务器不对经本服务器发送的邮件进行检查,也有可能造成邮件服务器发送垃圾邮件。

- ◆ 发信内容检查

如果邮件服务器的用户中存在恶意用户,利用本来用作正常商业邮件的服务器发送垃圾邮件。通过对发信内容的检查,可以有效拦截这些垃圾邮件。

- ◆ 蠕虫病毒检查

如果邮件服务器的用户感染了邮件蠕虫病毒,会在用户不知情的情况下,疯狂发送垃圾邮件和蠕虫病毒。对发信进行蠕虫病毒检查不但可以拦截这些垃圾邮件,而且也避免了进一步扩大蠕虫病毒的蔓延。

- ◆ 发信频率检查

垃圾邮件通常都是在短时间内高频率的大批量发送。正常的邮件(除许可邮件列表和用户确认的大宗邮件发送外)通常都是较低的发送频率。

- 邮件服务器的可靠性
 - 邮件投递可靠

邮件是否能够可靠的投递到收信人，不仅仅取决于对方的服务器的状况，还取决于以下几个方面之一或全部：

 - ◆ 服务器的 IP 地址状况
 - ◇ 是否被列入了黑名单
 - ◇ 是否有正确的反向解析
 - ◆ 服务器的发信人/发信域状况
 - ◇ 是否被列入了黑名单
 - ◇ 是否有正确的解析
 - ◆ 服务器的通讯协议是否标准
 - ◇ HELO/EHLO 的名称是否合理（FQDN）和是否存在
 - ◇ 支持的特性是否一致（如 PIPELINING）
 - ◇ MAIL FROM 是名称是否合理（FQDN）和是否存在
 - 邮件接收可靠

邮件服务器是否能可靠的接收邮件，主要取决于以下几个方面之一或全部：

 - ◆ 反垃圾邮件配置
 - ◇ 反垃圾邮件的设置可能过于严厉，拒收过多的正常信件
 - ◇ 反垃圾邮件可能悄悄丢弃了部分认定的垃圾邮件
 - ◇ 使用了过于武断或缺乏维护的黑名单
 - ◆ 并发处理能力
 - ◇ 接入带宽不足，不能快速处理发来的邮件
 - ◇ 服务器处理能力不足，不能快速处理发来的邮件
 - ◇ 并发连接的限制过小，不能同时处理多封邮件

通过邮件服务器的审计和对邮件服务器的用途及历史情况的分析，我们对邮件服务器进行可信级别的认证。

对邮件服务器认证后，我们会颁发认证证书，称之为 DSCA。DSCA 包括五个级别的证书：

- DSCA-1
经审计合格后，颁发给单 IP 或单服务器或单出口的普通企业级
- DSCA-2A
经审计合格后，颁发给单 IP 或单服务器或单出口的政府、事业、教育单位级
- DSCA-3A
经审计合格后，颁发给不超过 10 个 IP 或服务器的中小型运营商或中小企业
- DSCA-4A
经审计合格后，颁发给不超过 50 个 IP 或服务器的中型运营商或中型企业
- DSCA-5A
经审计合格后，颁发给不限制 IP 或服务器的中型运营商或跨国大企业

DSCA 的认证主要参考以下数据，并经过我们的数据模型进行运算生成：

- 邮件服务器的安全性
- 邮件服务器的可靠性
- 邮件服务器的用途
- 邮件服务器的历史发信情况

- 邮件服务器的使用程度、使用时间

通过可信级别的认证,可以让支持 Dr.SMTP 的 DSCA 的反垃圾邮件设备/软件能够更好的接收来自被认证的邮件服务器的邮件。目前,支持 Dr.SMTP 的 DSCA 的反垃圾邮件组织有 CASA (中国反垃圾邮件联盟),其发布的各种黑白名单中都会参考 Dr.SMTP 的 DSCA;此外,还有很多反垃圾邮件产品及组织也通过使用 CASA 的数据而间接参考了 Dr.SMTP 的 DSCA。

可以说, **经过了 Dr.SMTP 的认证,能有效提高邮件的顺利递交比例。**

3.5 DSL : Dr.SMTP Frequency Limit List

垃圾邮件高频率控制列表

Dr.SMTP 的 DSL 是一种针对**大量高频率发送邮件**进行控制的实时黑名单。有别于其它的实时黑名单,这种黑名单的刷新时间非常快,能有效防止在短时间内发送大量邮件的垃圾邮件行为。一般而言,垃圾邮件的发送都是在较短时间内完成,其在单位时间内发送的频率远远超乎正常的邮件递交频率(邮件列表发送也具有如此特征,但是我们针对合法的邮件列表发送做了必要的甄别),所以针对这样的高频率投递行为,对其进行软错误弹回,使其暂时不能投递,可有效避免垃圾邮件。正常的邮件递交,如果遇到软错误,会在一段时间后重试投递,不会影响邮件丢失;而垃圾邮件的发送在遇到软错误后,基本上不会进行重试投递。

根据我们的测算,DSL 的有效率(命中率)是一般垃圾邮件黑名单的两倍以上,可达到 50%以上的命中率。结合 CASA 其它的黑名单一同使用,可以获得更好的效果。

3.6 DSC : Dr.SMTP Consultation

邮件/反垃圾邮件技术咨询

作为邮件服务器的管理者,您需要很多的专业知识来管理和维护您的邮件服务。但是,邮件服务作为最常用也最早的 Internet 服务,其复杂性和多样性也非常令人困扰。当您遇到困难时,可以致电咨询我们,我们的专家组会协助您分析定位问题,并尽可能的提供最佳的解决方案。