

# Fortinet 反垃圾邮件解决方案

Fortinet 公司 赵彦利

在电子邮件应用普及的同时,垃圾邮件也在泛滥。由于邮件服务商无法有效控制垃圾邮件的发送或没有有效的约束手段,导致很多邮件服务商的 IP 地址被国外列入垃圾邮件黑名单。本文主要介绍邮件发送认证方法,以及 Fortinet 的集成型和独立型反垃圾邮件解决方案。

## 邮件发送认证体系

邮件系统本身没有安全机制,无法阻止垃圾邮件的收发。目前很多公司在致力于开发和推广新的邮件发送认证体系架构,帮助用户建立一个相对准确的邮件信誉系统,来完善邮件系统本身存在或无法解决的安全问题。

邮件发送认证方法目前主要有:SPF 发送者策略架构、Sender ID 及 Domain Key。

SPF 是最早采用的邮件发送者认证方式,它通过 DNS 来发布合法的某个域名发送邮件的地址或范围。邮件系统在接到邮件发送请求时,通过 DNS 查询该地址是否为合法的邮件发送地址,通过鉴别来决定是否接收该邮件。

Sender ID 是微软的邮件发送认证标准,是 SPF 的增强版本。虽然有些大的厂商和邮件服务商已经公开支持该标准,但由于涉及商业利益,很多厂商仍在观望。

Domain Key 是 Yahoo 的邮件认证标准,它在邮件发送连接时发送数字证书的认证信息,以此来提供更安全有效的认证方式。但很多厂商对这种邮件认证方法同样在观望。

目前反垃圾邮件厂商广泛采用多种方法来综合检测垃圾邮件,即所谓“鸡尾酒法”。通过采用优化统计的方法,根据某个特征贡献的分值再最终评判邮件的好坏。

目前常用的反垃圾邮件技术包括贝叶斯检测法、邮件头过滤、黑白名单、统计查询、实时黑洞列表查询、内容过滤。由于垃圾邮件的评判标准不一致,单一的邮件过滤策略对不同用户会有差异,这就给垃圾邮件的管理带来了压力。客户的要求是过滤垃圾邮件,但任何系统无法百分之百满足要求,因此所有垃圾邮件检测系统必须提供功能强大的邮件隔离管理系统。以此来有效杜绝垃圾邮件进入客户端邮件系统,同时又可以保证正常邮件不会丢失。

## Fortinet 反垃圾邮件策略和解决方案

Fortinet 是最早在统一威胁管理 (UTM) 系统中提供反垃圾邮件的厂商,其系列产品中都提供了反垃圾邮件的特性。Fortinet 在反垃圾邮件上提供两种不同的解决方案。集成的 FortiGate UTM 解决方案是在产品中提供了除贝叶斯之外的

所有垃圾邮件检测特性,为企业级客户提供全面的安全架构。同时, Fortinet 提供独立的反垃圾邮件系统 FortiMail。

FortiMail 是具有邮件服务器功能的邮件安全系统,它提供了强大的邮件安全防护机制,可以进行邮件病毒检测、IPS 防护、反垃圾邮件、内容安全过滤等功能。FortiMail 可以实现多种实施方案,包括代理模式、透明模式和服务器模式,可根据客户要求灵活部署。

代理模式 (Proxy) 模式通过修改 DNS MX 纪录部署新的邮件安全系统。客户需要对 DNS 进行必要的更新和修改。有些中小型企业由于自己没有 DNS 服务器,修改任何 DNS 纪录都要向 ISP 申请,可能需要一定时间,在部署时可能不方便。

透明模式是 FortiMail 的一个重要特性,它可以在不改变任何邮件系统网络的前提下,部署到邮件系统之前。该特性被众多用户所认可。

服务器模式是 FortiMail 系统的另外一个特性,它不但提供邮件安全的所有特性,同时提供具有全部邮件功能的邮件服务器。该功能可以为企业级客户提供极佳性价比的邮件服务器和邮件安全系统。FortiMail-400 型和 2000 型分别支持多达 1000 邮件用户和 3000 邮件用户,支持 Webmail, SMTP, POP3 和 IMAP 协议,安全的 (SSL) WebMail 客户端访问,基于用户的硬盘容量策略以及用于垃圾邮件的大容量文件夹。

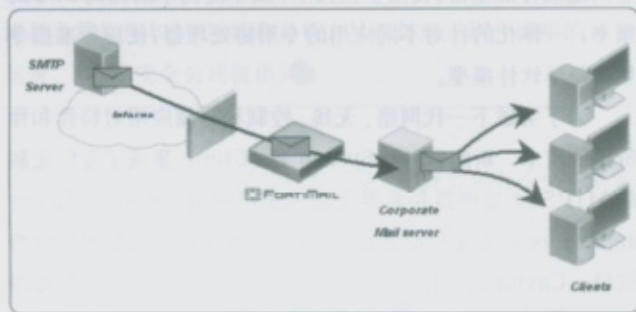


图 1 FortiMail 透明模式安全部署

Fortinet 的 FortiMail 安全消息平台具备完全内容检测能力,来检测最新的邮件威胁,提供企业级反垃圾邮件和防病毒性能,并具有最佳的配置灵活性,以确保关键性邮件应用。FortiMail-400 系统优化为中型规模的企业用户,以高可靠和高性能来检测、标签和阻挡垃圾信息和它们的有害附件。特点是快速安装、低维护开销和方便的管理界面,容易操作以及低成本的使用权。(本文作者赵彦利为 Fortinet 公司亚太区产品总监)