新软周报
HTTP WWW.NUSOFT.COM.TW
Internet Security Fighter
2009/7/13- 2009/7/26 第96期

邮件服務器 / ML 系列報導

技術淺談與應用 - 公司如何避免內對內信件傳送被誤判成垃圾郵件

在今日高度网络化的商业环境里，公司企业无不依赖电子邮件传递或收发大量商业讯息以维持组织运作，除了对外的联系之外，为了在每项作业都能有个重要的记录依据，于公司内部间的沟通也同样的早已将电子邮件用来做为最主要的管道之一。

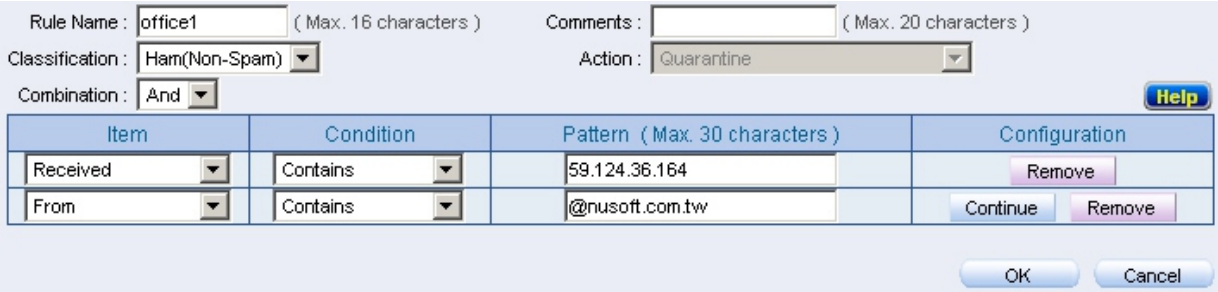
然而科技所带来的影响，除了创造了不少的便利之外同样也夹杂了不少的负面情况。垃圾邮件就是其中之一，现今垃圾邮件「污染」网络世界的情况到底多严重？这个问题相信在每个人心中都早已有了明确的答案。也正因为如此，企业纷纷的导入相关的资安防护设备，以维持正常运作。为解决扰人的垃圾邮件问题，新软系统所推出的『邮件服务器 - ML』，一直以来深受企业与公司的喜爱，正因为『邮件服务器 - ML』拥有了强大的防护功能以防止扰人的垃圾邮件再度来袭。

但垃圾邮件的欺骗手法也同样不断的在更新，发送者为了将信件送达至收件者信箱，其中一项手法则是利用伪造信件中的邮件地址来欺骗该公司邮件服务器中的过滤机制，让邮件服务器认为是公司里内部对内部之间所相互传送的信件而放行，因而造成公司内部人员不断的收到烦人的垃圾邮件。所以网络管理人员若是将公司内对内的信件皆设为无条件通行的情况，将有可能会因此而再一次的饱受垃圾邮件所困扰。为了避免这类的情形发生，该如何去设定邮件服务器上的阻挡规则，而最为重要的是又不会将内部所传送的信件误判为 SPAM 而遭阻挡才好呢？除此之外，于公司内，同事与同事间的信件传送，通常会单纯只以一个夹档的方式来寄送，而这样的方式和单纯只以单一图片之类的垃圾邮件寄送内容相似，以至于有可能会因此遭邮件服务器所阻挡，管理人员又该如何去解决？

首先，管理人员先进入“邮件安全 > 邮件过滤 > 全体化规则”，同时新增 2 项规则。

全体化规则内容第 1 项：

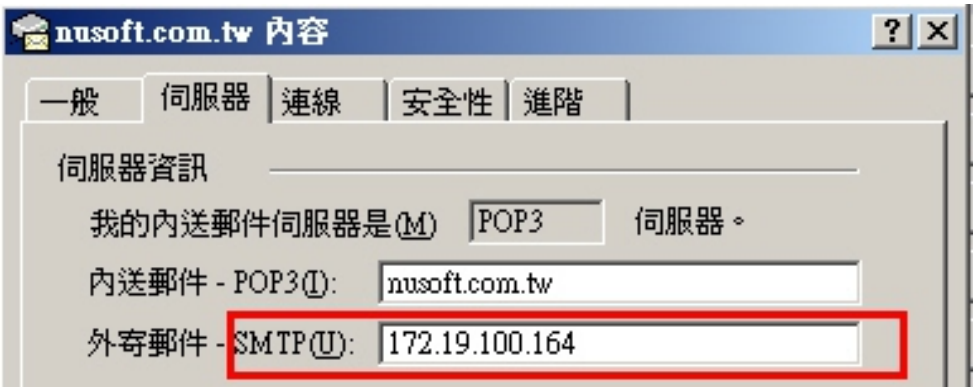
1. 将规则分类设为“Ham（Non-Spam）”。
2. 组合方式设为“And”。
3. 新增一条项目为“Received”、条件为“Contains”、邮件特征为“公司所设定的邮件服务器 IP”的规则条件。
4. 新增一条项目为“From”、条件为“Contains”、邮件特征为“公司所申请之 Domain name”的规则条件。



全體化規則設定範例圖片

全体化规则内容第 2 项：

1. 将规则分类设为“Ham（Non-Spam）”。
2. 组合方式设为“And”。
3. 新增一条项目为“Received”、条件为“Contains”、邮件特征为“公司内部(LAN)的网段 IP”的规则条件。(此条件为预防公司内部寄件者将 Outlook 中 SMTP 部份直接填为邮件服务器之 LAN 端 IP 地址，而非 Domain。因为若是直接填为邮件服务器之 LAN 端 IP 地址，在内部传送之信件所夹带的 IP 会是使用者本身计算机中 LAN 端 IP。)

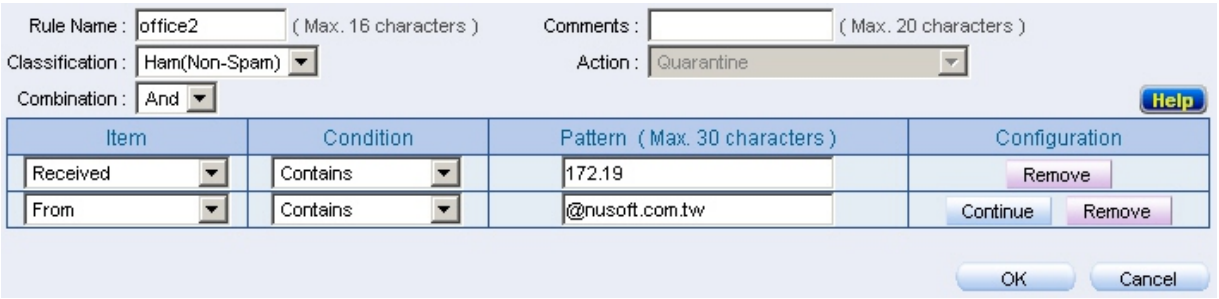


SMTP 所填內容為郵件服務器之 LAN 端 IP

```
Return-Path: <kim@nusoft.com.tw>
X-Original-To: kim@nusoft.com.tw
Delivered-To: kim@nusoft.com.tw
X-PushMail: kim:nusoft.com.tw:2:1|__D4ALL__:ALL:1:-10|
Received: from localhost.com.tw (unknown [172.19.50.9])
      by nusoft.com.tw (ML2000_164 XiM) with ESMTP
      for <kim@nusoft.com.tw>; Thu,  2 Jul 2009 20:00:48 +0800 (UTC)
Received: from K (unknown [172.19.50.9])
      by localhost.com.tw (Spam Filter XiS) with SMTP
      for <kim@nusoft.com.tw>; Thu,  2 Jul 2009 20:00:58 +0800 (UTC)
```

寄送之郵件所夾帶 IP 為使用者計算機內部 IP

4. 新增一条项目为“From”、条件为“Contains”、邮件特征为“公司所申请之Domain name”的规则条件。



全體化規則設定範例圖片

其如此设定的用义为何呢？因为发件者在伪造邮件位置来欺骗邮件服务器时，所能变动伪造的为『From』(下图红色框部份)，而『Received』来源位置(下图蓝框部份)是无法做更动的，所以当服务器收到信件后，判断条件须是利用『and』的方式，将『From』、『Received』两组条件皆符合该公司所设定之内容才能让该信件正常通过。

```
Return-Path: <rayearth@nusoft.com.tw>
X-Original-To: kim@nusoft.com.tw
Delivered-To: kim@nusoft.com.tw
X-PushMail: kim:nusoft.com.tw:2:1|__D4ALL__:ALL:1:-10|
Received: from localhost.com.tw (nusoft.com.tw [59.124.36.164])
      by nusoft.com.tw (ML2000_164 XiM) with ESMTP
      for <kim@nusoft.com.tw>; Mon, 22 Jun 2009 18:50:08 +0800 (UTC)
Received: from rayearth (nusoft.com.tw [59.124.36.164])
      by localhost.com.tw (Spam Filter XiS) with SMTP
      for <kim@nusoft.com.tw>; Mon, 22 Jun 2009 18:50:05 +0800 (UTC)
Message-ID: <01f601c9f327$3173b330$0201a8c0@rayearth>
From: "Rayearth" <rayearth@nusoft.com.tw>
To: "NUSOFT_陳殿鴻" <kim@nusoft.com.tw>
```

信件原始檔截圖

如此一来若是有心人士伪造邮件地址来欺骗邮件服务器以达到垃圾邮件的散播，则会因为没达到规则条件内容而无法顺利通过；反之，而当遇到真的是内部对内部之信件传送时，也不会因阻挡机制而遭『邮件服务器 - ML』误判为 SPAM，而错失掉重要的信件讯息。

文 陳殿鴻 kim@nusoft.com.tw

市場行銷報導 - 新軟「硬件式 Mail server」與一般「軟件式 Mail server」的差異

一般企业生意往来大多透过 Email 来传达所有的商业讯息，因此电子邮件对企业来说，其重要性自然不在话下。因此一间有规模、有制度的公司，必然得有一台可容易控管且功能强大的电子邮件服务器。

目前市场上以软件式 Mail Server 及硬件式 Mail Server 最为广泛使用。然而，很多人第一印象便是“我自己来架设软件式 Mail Server 应该会比较容易、省钱吧？”，其实不尽然。

《一般軟件式 Mail Server》：

一般软件式邮件服务器架设方式，无非是购入一台计算机硬件，然后安装操作系统，接着安置 Mail Server 软件、防毒软件…等等，最后再做相关设定及一连串的测试然后再实机上线。

这样的架设方式乍看之下难度似乎不高，其实并非如此。从技术层面来看：在系统建置时，首先就得面临使用哪个操作系统（Windows 或 Linux，若使用 Windows 虽然安装较容易，但是其版权成本极高且较耗系统资源，再加上容易成为黑客“照顾”的目标；若使用 Linux 虽然无需版权费用且安全性与稳定性较高，但是其安装时得对于 Linux 操作有专业的技术），接着面临 Mail Server 软件、防毒软件…等等成本及技术上的考虑，最后还得在后续维护成本上花不少的费用及时间和功夫，在种种问题解决后便将软件式 Mail Server 架设完成。

然而，这只是最原始功能之 Mail Server 而已，此时系统就像是堆积木一样地将各种所需元素堆积起来，若之后还需增加进阶功能时就得大幅变动系统之架构设计，管理人员所耗的时间就会越来越多，不可掌控的变量也就越来越多了，甚至容易使得系统因此而变的更为脆弱。

《新軟硬件式 Mail Server》：

新软系统所推出的硬件式邮件服务器 - ML 系列，贯彻「轻松架设、功能完整、维护简单」此设计理念。在硬件上以安全、稳定的嵌入式 Linux 系统为核心平台。在软件上，以简单、人性化的操作接口呈现于管理者面前，无须丰富的专业知识也可以轻松架设。

在相关邮件服务、稽核等功能上也一应俱全，另外拥有独家账号信件无痛移植功能，取代企业原有邮件服务器，快速方便且可以与 LDAP 服务器搭配结合做完整账号整合。在防毒机制上也以 ClamAV 等两种扫毒机制严阵以待。而针对变化性极大的 SPAM 垃圾信，新软以包含独家提供的「垃圾邮件特征码」在内的七道垃圾邮件过滤机制，彻底扫荡垃圾邮件。在备援机制问题上，以独家的 HA 双主机备援方式用以确保系统内所有数据的备援完整性。其它包含业务部门较常用的「Push Mail」、「WebMail」等功能也都贴心地建构于其中。

最后令公司企业最为关心的就是「系统后续维护成本」，新软对产品用户提供了完善的售后服务，对于垃圾邮件特征码、ClamAV 扫毒引擎病毒码等更新服务上，皆不收取任何的费用。

新软系统所推出之硬件式邮件服务器 - ML 系列不单单只是一台会收发信件的机器而已；更重要的是它带来更多更强大功能、更方便之操作接口以及减少后续维护时所花费的精神、时间、成本。如此一来，Mail Server 才能真正达到现代企业的完整需求。

	新軟硬件式 Mail server - ML 系列	一般軟件式 Mail server
軟硬件成本	低	高
建構技術成本	低	高
人力花費成本	低	高
后續維護成本	低	高
防毒防駭安全性	高	低
多樣強大功能	高	低
完整售后服務	有	無

新軟硬件式郵件服務器 - ML 系列與一般軟件式 Mail Server 差異表。

文 黃政銘 ming@nusoft.com.tw