新软周报
http://www.nusoft.com.tw
Internet Security Fighter
2007/7/2 - 2007/7/8 第32期

多功能 UTM / MS 系列报导

技术浅谈与应用 - 多功能 UTM 防毒机制介绍（ Mail、Policy、IDP ）

网络方便的运用在商业往来的各种环境中，无不促使产业蓬勃发展。在这看似正面且能带来大量效益的讯息传递环境中，却有人为了利益或其它意图刻意散布危及整体网络使用人权益的病毒程序，小则造成个人用户使用的不便，大则造成网络的瘫痪、重要机密被窃、存盘数据遗失…。

为了因应堪称网络蝗灾的病毒程序，早期用户只能在 PC 安装防毒软件以求自保。但常因为个人的疏忽而久未更新病毒码，造成无法达到实际保护作用。而一般防火墙仅能针对各项网络服务拦阻，无法防御来自病毒的危害。

有鉴于此，新软多功能 UTM 针对各式各样的网络服务建置了数种病毒扫描机制。以新软 NUS-MS3500 来说，针对网络数据传输做的病毒侦测动作，可分为下列数种：

- 邮件病毒过滤－

一般来说，最大的病毒扩散管道就是透过电子邮件传输。当邮件传递时，NUS-MS3500 会先行将其存放于一暂存区，并针对信件的内容、所夹带的文件扫毒（压缩档解压扫毒）。若邮件判断为异常（病毒邮件、钓鱼邮件...），NUS-MS3500 会将该邮件依照管理人员所设定的处置方式处理（隔离储存、删除...）剩下的邮件再交由垃圾邮件过滤机制处理。

- HTTP / Web Mail、FTP 病毒过滤－

以网页方式散拨病毒、木马、间谍程序...是目前黑客最喜欢的作法。常常可听到某网站被黑客入侵，并在其网页中植入恶意程序的消息。由于这些网站包含有电视台、医院、企业厂商、学校、政府机构...这些知名单位、厂商，所以一般使用者根本不会考虑这些网站是否有问题而疏于防范。

NUS-MS3500 拥有 HTTP、FTP 病毒过滤功能。管理人员可在制定网络管理政策（Policy）时，启用内建的病毒侦测功能。使用者在上网时 NUS-MS3500 会将透过 HTTP（包含 Web Mail）、FTP 服务传输的文件，先行下载于一暂存区并进行扫毒动作。将判别有异的文件直接阻绝并删除，正常的文件则由暂存区中提取出来，传送到目的端。

• IDP 病毒过滤－

至于其它网络服务的病毒要如何防范呢？利用实时通讯传递文件、P2P下载软件...这也是一般使用者会使用的网络行为。管理人员可以使用 NUS-MS3500 内建的 IDP 病毒过滤机制，针对往来的封包，逐一比对其所包含的数据是否有病毒特征，来达到病毒防护的效果。将判别有异的封包直接阻绝，并终止该联机后续封包的传送，无异常封包的联机则可持续完成传送到目的端的动作。

	病毒邮件扫描	管制条例（Policy）HTTP、Web Mail、FTP 扫毒机制	IDP 病毒侦测
采用的扫毒引擎	Clam、Sophos	Clam、Sophos	Clam
扫描文件的方式	先行储存於一暂存区，对邮件夹带的未加密文件直接扫毒、压缩档解压扫毒	先行储存於一暂存区，对传输的未加密文件直接扫毒、压缩档解压扫毒	针对传输文件的封包，检查是否有病毒特徵

文 陈昱升 josh@nusoft.com.tw

市场营销报导 - 防毒引擎 ClamAV 与 Sophos 之差别

在这计算机病毒泛滥的时代，网页、电子邮件、实时通讯软件...都已成为病毒感染的途径。计算机极易因为使用者的疏忽而中毒，造成无法弥补之损失。为此企业通常会架设防毒系统来保护其网络、数据之安全。

一般企业的防毒系统建置，除了在每台计算机上都安装防毒软件之外，另一种作法就是建构一个拥有防毒机制的网关器（防毒墙），来过滤企业往来之封包。以防毒网关器的方式来防护企业网络，可将病毒阻绝于企业网络之外，不让它有任何机会进入企业网络，且其建置经费也较低于企业全面安装防毒软件。因此，建置防毒网关器也渐渐企业防毒机制的主流选项。

为了顺应此潮流，新软系统所推出的多功能 UTM 内建了两种扫毒引擎：ClamAV 与 Sophos 供企业选择。企业可单独选用其中一款扫毒引擎来防御企业网络。甚至也可让 Sophos 与 ClamAV 同时运作，提供企业网络双重保障。

ClamAV－（NUS-MS3500、NUS-MS2000A、NUS-MS1500、NUS-MS700）

ClamAV 目前可以侦测超过四万种病毒、蠕虫以及木马程序。并有一群分布在世界各地的计算机病毒专家，24 小时的随时在在线更新及维护病毒数据库。如有新型病毒出现，可立刻反应，并发布新病毒码。届时，透过新软多功能 UTM 内建的自动在线更新系统（每十分钟在线搜寻一次），即可取得最新病毒码。

与其它商业防毒软件需每年付费授权与使用人数有所限制不同的是，新软多功能 UTM 所内建的 ClamAV 可永久免费更新病毒码，而且并无使用人数限制。这可让新软多功能 UTM 的病毒防护功能，能以最少的成本，永远保持在最新的状态。

或许有人会怀疑，新软多功能 UTM 所内建之扫毒引擎采取免费更新病毒码的方式是否可靠，是否能永续服务下去。事实上，ClamAV 采取与 Linux 相同的运作模式：公开程序代码以及免费授权。因此，其安全性已接受过全球无数计算机工程师的检验，可确定安全无虞。再加上全世界已有无数个网站提供 ClamAV 在线病毒码更新。如此汇聚众人的力量，成就免费而且永续的网络服务。

Sophos－（NUS-MS3500、NUS-MS2000A、NUS-MS1500）

如果使用者无法相信免费的扫毒引擎，新软多功能 UTM 亦提供了一套欧洲的著名的商业扫毒引擎－ Sophos。Sophos 为出自英国的防毒引擎品牌，拥有多项病毒分析之专利，可以有效侦测各种病毒、蠕虫、木马程序...有害程序。质量受到各界的肯定（获得 Information Security 杂志 2004 年度资安风云产品金奖）。

Sophos 在英国、美国、澳洲均设有病毒研究中心，全年二十四小时随时更新病毒数据库。新软多功能 UTM 只需透过内建的自动在线更新系统（每十分钟在线搜寻一次），即可自动更新病毒码，完全不需管理人员手动更新。

06:42	Clam AV	06:51	Kaspersky	08:21	Bitdefender
08:45	Virusbuster	09:08	F-Secure	09:16	F-Prot
09:16	RAV	09:24	AntiVir	10:31	Quickheal
10:52	InoculateIT-CA	11:30	Ikarus	12:00	AVG
12:17	Avast	12:22	Sophos	12:31	Dr. Web
13:06	Trend Micro	13:10	Norman	13:59	Command
14:04	Panda	17:16	Esafe	24:12	A2
26:11	McAfee	27:10	Symantec	29:45	InoculateIT-VET
单位— 小时：分钟				Virus：MyDoor.s	

表一 各家防毒业者对新病毒的反应速度

文 程智伟 rayearth@nusoft.com.tw