新软周报
http://www.nusoft.com.tw
Internet Security Fighter
2008/1/28-2008/2/3 第60期

负载均衡器 / MH 系列报导

技术浅谈与应用 - Log 的种类及功能（二）

延续第 59 期周报『Log 的种类及功能（一）』的内容，我们将继续介绍其它新软系统多功能 UTM（MS 系列）及负载平衡器（MH 系列）产品内建的 Log 种类与功能：

四、IM/P2P Blocking Log：

在阅览『IM/P2P Blocking Log』之前，网管人员必须先在管制条例（Policy）内的「IM/P2P Blocking」规则做设定。ex：网管人员在管制条例中的 IM/P2P Blocking 功能新增一条”阻挡 MSN 登入及 Edonkey 软件禁止使用”的规则后，当使用者在使用 MSN 及 Edonkey 软件时，不仅会发现无法登入 MSN 及使用 Edonkey 下载文件外，同时『IM/P2P Blocking Log』也会同步记录「哪位员工（来源计算机名称 or IP 地址）」、「什么时候」、使用哪套「IM/P2P 软件」或「利用哪套 IM 软件传送文件」。透过『IM/P2P Blocking Log』，可使网管人员与企业决策者清楚得知旗下员工是否在上班时间私自使用 IM/P2P 软件的情形。

Time	Source IP	IM / P2P
Jan 15 16:58:15	AJ	QQ
Jan 15 16:55:18	ABC	Gadu-Gadu
Jan 15 12:35:14	JOSH12	Thunder5
Jan 15 10:13:59	OWEN104	Edonkey
Jan 14 16:22:25	SIMSAN	QQ FILE TRANSFER

图一 『IM/P2P Blocking Log』记录内容

五、Content Blocking Log：

在检阅『Content Blocking Log』之前，网管人员必须先在管制条例（Policy）内的「Content Blocking」规则做设定。网管人员在管制条例中的 Content Blocking 新增一条限制浏览网址列上含有「yahoo」字眼的所有网页（奇摩拍卖 bid. yahoo. com、奇摩首页 yahoo. com、奇摩新闻 news. yahoo. com. . .）及禁止所有扩展名为影像相关（mp3、mpeg、rmvb. . .）的文件下载之管制规则。

此时只要使用者浏览网址列上有着「yahoo」字眼的网页，全部都将无法显示；而使用者从HTTP、FTP下载影音文件时，也将发现影音相关的文件均无法下载。在上述情况发生的同时，『Content Blocking Log』也会同步将使用者的这些行为详细记录下来。透过『Content Blocking Log』，网管人员可清楚得知是「哪位员工」在「什么时间」到「哪个地方（Web网页、FTP站台...）」进行「什么事情（浏览网页、从HTTP或FTP下载文件...）」，进而管制及掌握企业员工的网页浏览与文件下载情形。

Time	Source	Destination	Protocol	Port	Type
Jan 16 11:40:11	192.168.168.16	202.43.195.52	TCP	1977 => 80	URL
Jan 16 11:40:15	192.168.168.59	202.43.195.52	TCP	1982 => 80	URL
Jan 16 11:41:12	192.168.168.104	69.80.230.44	TCP	1565 => 80	Download
Jan 16 11:41:22	192.168.168.52	140.127.177.17	TCP	2019 => 21	Download
Jan 16 11:41:23	192.168.168.230	140.128.9.18	TCP	2021 => 21	Download

图二 『Content Blocking Log』记录内容

六、Virus Log：（只有NUS-MS系列产品才有此功能）

在查看『Virus Log』之前，网管人员须先启用管制条例（Policy）内的「Anti-Virus」规则（图三）。当使用者透过HTTP、Web Mail或FTP下载文件时，若下载文件含有病毒时，系统除了会主动侦测出含有病毒的文件名称、类型与病毒种类，同时加以阻档拦截其下载动作，并将信息同步更新至『Virus Log』上。透过『Virus Log』，网管人员可得知使用者从哪些网站或服务器下载到含有病毒的文件，进而针对这些病毒来源网站进行封锁管制的动作，以防文件病毒危害到企业网络与个人数据的安全。

图三 管制条例（Policy）内的病毒防护功能

Time	Source IP	Destination IP	Protocol	Download File	Virus Name
Jan 23 12:53:07	192.168.1.21	cn.yimg.com	HTTP	cs0619.exe	MalBehav-053
Jan 23 12:53:06	192.168.1.28	www.asm.com	HTTP	jt.exe	MalBehav-156
Jan 23 12:53:06	192.168.1.24	nx.51ylb.cn	HTTP	mh2.exe	MalBehav-031
Jan 23 12:53:05	192.168.1.28	cn.yimg.com	HTTP	qqsg.exe	MalEncPk-BW
Jan 23 12:53:04	192.168.1.24	123.wwwwool.cn	HTTP	dh3.exe	MalPWS-N

图四 『Virus Log』记录内容

介绍这么多种类的 Log，大家可以轻易的发现，新软系统多功能 UTM（MS 系列）及负载平衡器（MH 系列）所提供的 Log，无论是信息提供的详细度、功能性及判读难易都不是一般网络设备提供的 Syslog 所能望其项背的。在企业每秒必争的网络环境上，当公司网络突然中断、服务器遭受不明流量攻击或网络设备不知为何当机导致无法运作等突发状况，网管人员如何在第一时间取得关键信息来实时处理危机状况！？此时，Log 的重要性就不言而喻了。

文 黄赞中 isaac@nusoft.com.tw

市场营销报导 - 两条外线可带来什麼好处

随着网络科技发展至今，宽带网络的费用日渐降低，人人拥有大带宽、高稳定的宽带线路来架设服务器不再只是梦想。单一线路已不能满足现代人时常大量存取网络资源的需求，两条外线才能提供中小企业及 SOHO 稳定的网络服务，无论是架设服务器提供服务，或者是上网存取网络资源，透过两条外线可让企业网络与因特网的传输更顺畅。

对企业来说，两条外线不仅能分摊企业网络的流量，也可供企业规划网络行为的流向分配，例如规画服务器由第一条外线连上因特网提供服务，一般上网行为则由第二条外线传输。藉由两条外线以维持企业网络对外的服务以及其它网络行为的传输质量。但是，若没有设置任何一个设备来管理企业网络与这两条外线的运作，那么两条外线所能提供的功能将会遭受限制而较无弹性，在调整流量的分配上也较为不便。

新软多功能 UTM（Multi Security UTM）以及新软负载平衡器（Multi Homing Gateway）均拥有多个 WAN Port 可支持两条以上外线，提供「负载平衡」、「带宽分流」、「断线备援」等功能，将此产品设置于企业网络对外的出入口，便能统一控管企业网络对内对外的封包流向，不仅享有两条外线的优点，并且能依照企业内部每个使用者、服务器、网络行为等条件，分配外线使用。

使用新软多功能 UTM 或新软负载平衡器搭配两条外线可带来什麼好处：

1.负载平衡：
可将企业网络与因特网间的传输流量分均分摊于两条外线，使得网络传输畅通，不至于发生其中一条外线流量过大造成阻塞，而另一条外线则不常运作而造成浪费。

2.带宽分流：
可因使用者、网络行为、服务种类...等条件，制定管理规则使该流量依循规则只通过其中的一条外线。这个功能的好处是若有需要保持某种网络服务的质量（例如 VOIP 的影音服务），那么便可以规划将此服务的流量与其它流量分别配置于两条外线，如此一来该网络服务就不会因其它网络行为所造成的大流量而影响质量。

3.断线备援：
两条外线的好处在于当其中一条外线断线，另外一条外线即会背负起企业网络的所有流量，维持网络的联机。假设与客户透过网络商讨会议，就算其中一条外线断线，也能继续维持网络会议的进行。

文 黄智杰 alex@nusoft.com.tw