新软周报
http://www.nusoft.com.tw
Internet Security Fighter
2008/1/21-2008/1/27 第59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（一）

市面上常见防火墙设备内建的记录文件（Log）包含了许多信息，举凡机器内部运作的事件日志、对内/对外的联机记录日志、IM/P2P 软件阻挡的记录日志...内容包罗万象、种类繁多，如果在没有归类的情形之下，企业 IT 人员还未找出系统发生问题的症结、对外联机中断的肇因…之前，就已经被庞大的数据给吞噬了！

新软系统所推出的多功能 UTM（MS 系列）及负载平衡器（MH 系列）产品内建的日志（Log）功能颠覆一般传统防火墙设备的单一 Syslog 记录方式，将不同的工作事件、联机记录分门别类，使 IT 人员能轻松地、直觉性判断其种类与内容；同时，在 Log 浏览接口上还提供亲切的下载及远程备份服务，这样贴心的功能在市面上可说是相当别出心裁。

下面将介绍新软系统多功能 UTM（MS 系列）及负载平衡器（MH 系列）产品内建的 Log 种类：

一、Traffic Log：

首先我们从『Traffic Log』来为大家做介绍，在『Traffic Log』的内容上，网管人员可透过清楚简单的记录显示得知内部员工「什么时候（日期、时间）」、「从哪个地方（来源 IP 地址）」、「到哪些远程设备（目的 IP 地址）」、「从事什么类型的网络活动（封包传送采用的协议）以及所传输使用的网络流量（只有 NUS-MS 系列产品才有，如图一）」。从『Traffic Log』中，如有外部使用者正在攻击架设于 NUS-MS、MH 系列产品底下的邮件服务器时，透过内建的『Traffic Log』机制，网管人员可直接观察到其攻击事件记录，进而做实时应对处理（图二）。

Time	Source IP	Destination IP	Protocol	Port	Traffic	Disposition
Jan 16 16:26:46	218.165.76.241	168.95.1.1	TCP	46217 => 80 (WAN1)	92 B	✓
Jan 16 16:26:46	172.19.100.82	220.132.12.146	TCP	2705 => 443 (WAN2)	171 KB	✗
Jan 16 16:26:46	218.165.76.241	61.189.163.4	TCP	46218 => 80 (WAN1)	60 B	✓
Jan 16 16:26:46	172.19.100.85	24.30.199.7	ICMP	--- (WAN1)	168 B	✓
Jan 16 16:26:46	80.24.113.86	59.124.36.163	TCP	19152 => 80 (WAN1)	60 B	✓

图一 『Traffic Log』记录内容

Time	Source IP	Destination IP	Protocol	Port	Disposition
Jan 16 11:47:47	69.80.230.44	192.168.1.1	TCP	33518 => 25 (in:WAN1)	✓
Jan 16 11:46:59	69.80.230.44	192.168.1.1	TCP	28946 => 25 (in:WAN1)	✓
Jan 16 11:46:35	69.80.230.44	192.168.1.1	TCP	2011 => 25 (in:WAN1)	✓
Jan 16 11:46:23	69.80.230.44	192.168.1.1	TCP	2018 => 25 (in:WAN1)	✓
Jan 16 11:46:17	69.80.230.44	192.168.1.1	TCP	5050 => 25 (in:WAN1)	✓

图二　某来源 IP 针对 192.168.1.1 这台邮件服务器的 25 port（SMTP）进行连续性联机，且不断变换传输 port，行为相当诡异，疑似遭到攻击

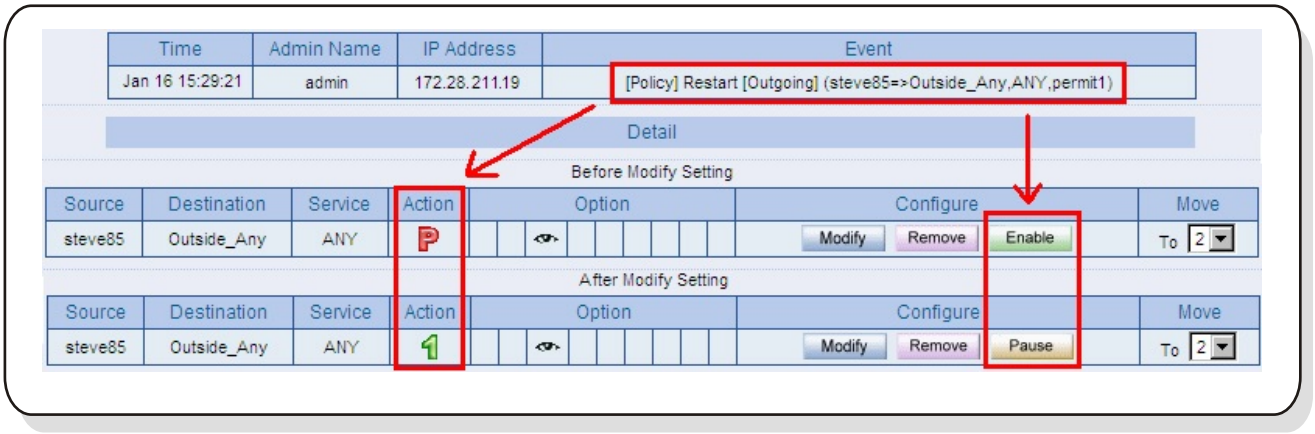
二、Event Log：

而『Event Log』主要记录新软系统多功能 UTM（MS 系列）及负载平衡器（MH 系列）产品内部所发生的事件，ex：使用者登入、管制条例（Policy）规则变动、韧体更新...。当使用者登入系统进入管理者接口时，『Event Log』会同步将这位使用者的「来源 IP 地址」、「登入账号」、「登入时间」与「登入成功 or 失败的讯息」详细记录于 Log；而系统韧体变更时，也可透过『Event Log』清楚得知是「哪位使用者」、「在什么时候」、「将韧体变更为哪个版本」等相关讯息。

而 Policy 管制条例有所更动时，『Event Log』机制不仅会在表格上显示相关概要外（哪位使用者与变更什么规则等信息），更将管制条例”变更前”及”变更后”的信息「图形化」并整合在同一张图片中，让网管人员能更加一目了然得知变动时的相关信息，相当方便好用。透过『Event Log』不仅让 MIS 人员能轻松掌握机器的运作状况与人员进出管理接口及设定情形，图形化的表示方式在市场上不仅少见，同时也相当受到企业厂商的青睐！

Time	Admin Name	IP Address	Event	Detail
Jan 16 15:29:21	admin	172.28.211.19	[Policy] Restart [Outgoing] (steve85=>Outside_Any,ANY,permit1)	📁
Jan 16 15:09:19	guest	211.75.117.114	[Login success]	-
Jan 16 15:08:08	admin	61.228.179.66	[Policy] Delete [Outgoing] (simsan=>Outside_Any,ANY,permit2)	📁
Jan 16 14:59:02	admin	172.28.211.100	[Login success]	-
Jan 16 14:55:59	guest	123.112.69.121	[Login failure]	-

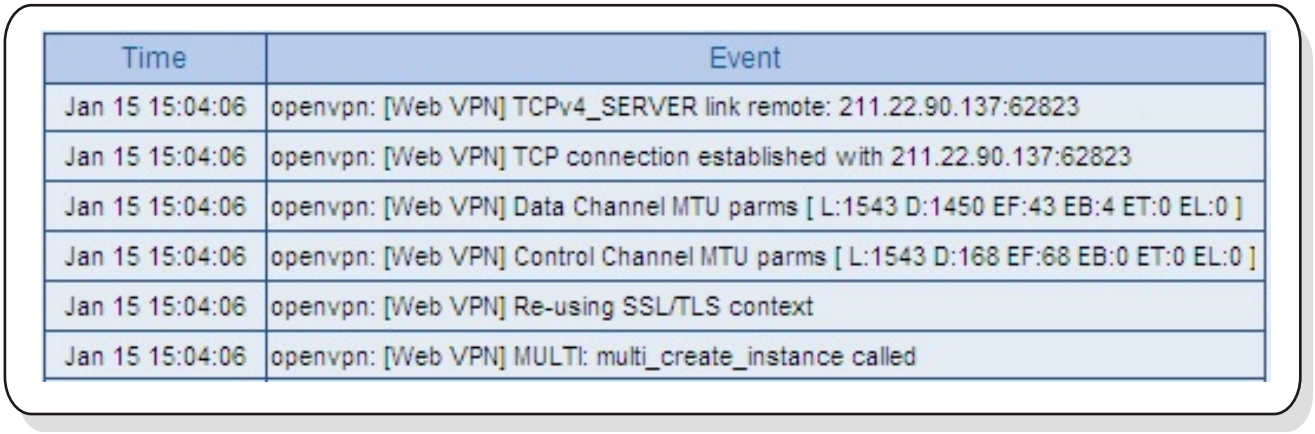
图三 『Event Log』记录内容



图四 一目了然的『Event Log』图形化表达方式

三、Connection Log：

『Connection Log』主要在记录透过机器联机 or 计算机联机至此机器的事件记录，ex：当使用者透过新软系统多功能 UTM（MS 系列）或负载平衡器（MH 系列）产品建立 VPN 联机时，『Connection Log』会详细记载联机时的相关信息，当无法建立 VPN 联机时，也可透过『Connection Log』来分析、侦错问题的原因



Time	Event
Jan 15 15:04:06	openvpn: [Web VPN] TCPv4_SERVER link remote: 211.22.90.137:62823
Jan 15 15:04:06	openvpn: [Web VPN] TCP connection established with 211.22.90.137:62823
Jan 15 15:04:06	openvpn: [Web VPN] Data Channel MTU parms [L:1543 D:1450 EF:43 EB:4 ET:0 EL:0]
Jan 15 15:04:06	openvpn: [Web VPN] Control Channel MTU parms [L:1543 D:168 EF:68 EB:0 ET:0 EL:0]
Jan 15 15:04:06	openvpn: [Web VPN] Re-using SSL/TLS context
Jan 15 15:04:06	openvpn: [Web VPN] MULTI: multi_create_instance called

图五 VPN 联机时的『Connection Log』

将新软系统多功能 UTM（MS 系列）及负载平衡器（MH 系列）产品提供的 Log 机制与坊间一般网络设备提供的 Syslog 机制互相比较之下，明显地发现，不仅信息记录的详细性与可读性都不是一般网络设备内建的 Log 所能比拟的，同时此功能对于网管人员来说可是相当地受用喔！

另外，新软系统多功能 UTM（MS 系列）及负载平衡器（MH 系列）产品所提供的 Log 种类可不是只有上面介绍的三种而已喔！我们将在第 60 期「Log 的种类及功能（二）」的周报内容中为大家介绍更多的 Log 种类以及功能说明。

文 黄赞中 isaac@nusoft.com.tw

市场营销报导 - 为何企业不适用低价 IP 分享器的理由

市面上网络设备玲珑满目，从百元至百万元的商品都有，当 IP 不够使用的时候，第一个会想到的或许是以 IP 分享器来解决问题，对一般家庭来说，IP 分享器是个经济又实惠的选择，但对于有众多需求的企业来说，使用一般的 IP 分享器是否真的合适呢？

一般低价的 IP 分享器只将实体 IP 以 NAT（Network Address Translation）的方式将实体 IP 分为多个虚拟 IP 供给内部 PC 使用，并提供 Port Mapping 的功能让内部的服务器得以运作。但仅有这些功能并无法满足企业的需求，由于企业网络规划复杂，不仅需要让每个 User 都能上网，更需要设定一些企业网络的管理规则，才能在有秩序的网络系统下达到企业所需的网络服务，甚至企业拥有多条对外实体线路，需要负载平衡的机制；而这些功能并不是一般 IP 分享器能够供给的，需要更多的网络设备与 IP 分享器一同搭配才有办法达到这个目标，但这样的设备组合所费不赀，所以一般低价的 IP 分享器并不适用于企业对象。

新软 Multi-Homing Gateway 不仅包含了一般 IP 分享器的功能，更具备了企业在网络管理上的需求，提供多项功能设定，将众多的网络设备整合在一起，包含多线路负载备援、带宽管理、防火墙、IM/P2P 管理、VPN 设定...等许多强大功能，例如公司须把 VOIP 与一般上网线路做分流并限制使用带宽，又可能需要与分公司建立 VPN 存取之间的内部数据，这些企业大都需要使用到的功能并不是一般低价的 IP 分享器能够提供的，另外若公司内部有大量的 PC 在使用网络，透过一般的 IP 分享器将会使的网络联机非常不稳定，而这些问题与需求只要一台新软 Multi-Homing Gateway 便可解决，不仅所需的花费比买齐了所有功能的众多设备还省，所占的空间更是小了许多。

企业不适用低价 IP 分享器的理由：

1. 功能性不足。
2. 无法应付多台 PC 同时上网。
3. 扩充其它设备增加所需功能需付出更多的花费，且占用更大的空间。
4. 扩充其它设备增加所需功能，必须针对各个设备做设定非常不方便。

文 黄智杰 alex@nusoft.com.tw