新軟週報
http://www.nusoft.com.tw
Internet Security Fighter
2008/1/21-2008/1/27 第59期

負載平衡器 / MH 系列報導

技術淺談與應用 - Log 的種類及功能（一）

市面上常見防火牆設備內建的記錄檔（Log）包含了許多資訊，舉凡機器內部運作的事件日誌、對內/對外的連線記錄日誌、IM/P2P 軟體阻擋的記錄日誌...內容包羅萬象、種類繁多，如果在沒有歸類的情形之下，企業 IT 人員還未找出系統發生問題的癥結、對外連線中斷的肇因…之前，就已經被龐大的資料給吞噬了！

新軟系統所推出的多功能 UTM（MS系列）及負載平衡器（MH 系列）產品內建的日誌（Log）功能顛覆一般傳統防火牆設備的單一 Syslog 記錄方式，將不同的工作事件、連線記錄分門別類，使 IT 人員能輕鬆地、直覺性判斷其種類與內容；同時，在 Log 瀏覽介面上還提供親切的下載及遠端備份服務，這樣貼心的功能在市面上可說是相當別出心裁。

下面將介紹新軟系統多功能 UTM（MS 系列）及負載平衡器（MH 系列）產品內建的 Log 種類：

一、Traffic Log：

首先我們從『Traffic Log』來為大家做介紹，在『Traffic Log』的內容上，網管人員可透過清楚簡單的記錄顯示得知內部員工「什麼時候（日期、時間）」、「從哪個地方（來源 IP 位址）」、「到哪些遠端設備（目的 IP 位址）」、「從事什麼類型的網路活動（封包傳送採用的協定）以及所傳輸使用的網路流量（只有 NUS-MS 系列產品才有，如圖一）」。從『Traffic Log』中，如有外部使用者正在攻擊架設於 NUS-MS、MH 系列產品底下的郵件伺服器時，透過內建的『Traffic Log』機制，網管人員可直接觀察到其攻擊事件記錄，進而做即時應對處理（圖二）。

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	✓

圖一 『Traffic Log』記錄內容

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)	✓

圖二　某來源 IP 針對 192.168.1.1 這台郵件伺服器的 25 port（SMTP）進行連續性連線，且不斷變換傳輸 port，行為相當詭異，疑似遭到攻擊

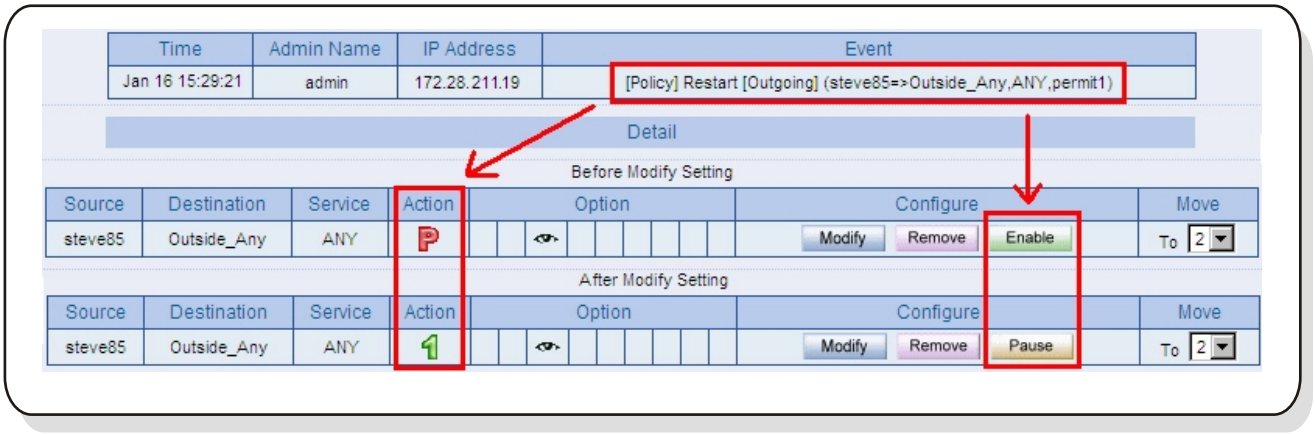
二、Event Log：

而『Event Log』主要記錄新軟系統多功能 UTM（MS 系列）及負載平衡器（MH 系列）產品內部所發生的事件，ex：使用者登入、管制條例（Policy）規則變動、韌體更新...。當使用者登入系統進入管理者介面時，『Event Log』會同步將這位使用者的「來源 IP 位址」、「登入帳號」、「登入時間」與「登入成功 or 失敗的訊息」詳細記錄於 Log；而系統韌體變更時，也可透過『Event Log』清楚得知是「哪位使用者」、「在什麼時候」、「將韌體變更為哪個版本」等相關訊息。

而 Policy 管制條例有所更動時，『Event Log』機制不僅會在表格上顯示相關概要外（哪位使用者與變更什麼規則等資訊），更將管制條例”變更前”及”變更後”的資訊「圖形化」並整合在同一張圖片中，讓網管人員能更加一目瞭然得知變動時的相關資訊，相當方便好用。透過『Event Log』不僅讓 MIS 人員能輕鬆掌握機器的運作狀況與人員進出管理介面及設定情形，圖形化的表示方式在市場上不僅少見，同時也相當受到企業廠商的青睞！

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]	-

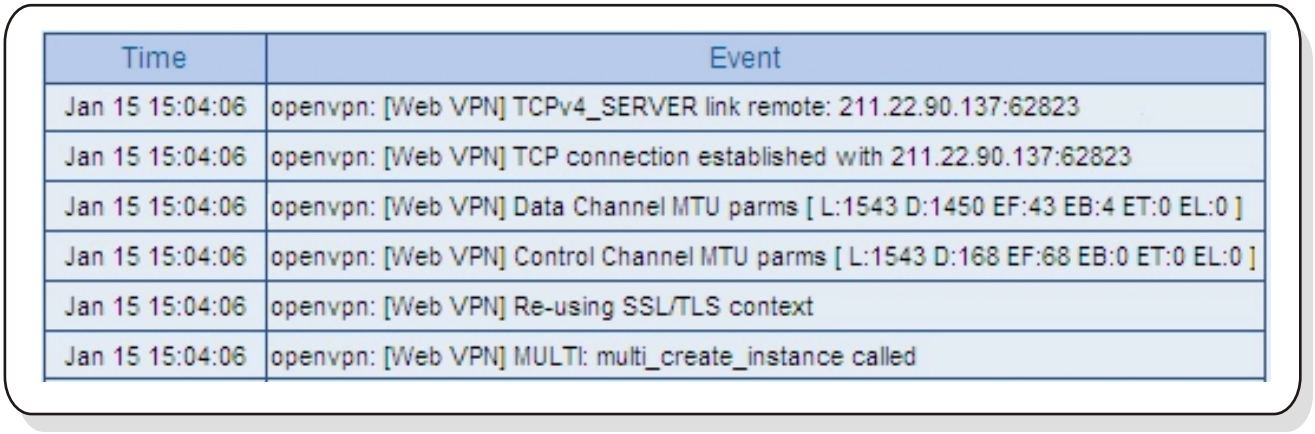
圖三 『Event Log』記錄內容



圖四 一目瞭然的『Event Log』圖形化表達方式

三、Connection Log：

『Connection Log』主要在記錄透過機器連線or電腦連線至此機器的事件記錄，ex：當使用者透過新軟系統多功能 UTM（MS 系列）或負載平衡器（MH 系列）產品建立 VPN 連線時，『Connection Log』會詳細記載連線時的相關資訊，當無法建立VPN連線時，也可透過『Connection Log』來分析、偵錯問題的原因。



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

圖五 VPN 連線時的『Connection Log』

將新軟系統多功能 UTM（MS 系列）及負載平衡器（MH 系列）產品提供的 Log 機制與坊間一般網路設備提供的 Syslog 機制互相比較之下，明顯地發現，不僅資訊記錄的詳細性與可讀性都不是一般網路設備內建的 Log 所能比擬的，同時此功能對於網管人員來說可是相當地受用喔！

另外，新軟系統多功能 UTM（MS 系列）及負載平衡器（MH 系列）產品所提供的 Log 種類可不是只有上面介紹的三種而已喔！我們將在第 60 期「Log 的種類及功能（二）」的週報內容中為大家介紹更多的 Log 種類以及功能說明。

文 黃贊中 isaac@nusoft.com.tw

市場行銷報導 - 為何企業不適用低價 IP 分享器的理由

市面上網路設備玲瓏滿目，從百元至百萬元的商品都有，當 IP 不夠使用的時候，第一個會想到的或許是以 IP 分享器來解決問題，對一般家庭來說，IP 分享器是個經濟又實惠的選擇，但對於有眾多需求的企業來說，使用一般的 IP 分享器是否真的合適呢？

一般低價的 IP 分享器只將實體 IP 以 NAT（Network Address Translation）的方式將實體 IP 分為多個虛擬 IP 供給內部 PC 使用，並提供 Port Mapping 的功能讓內部的伺服器得以運作。但僅有這些功能並無法滿足企業的需求，由於企業網路規劃複雜，不僅需要讓每個 User 都能上網，更需要設定一些企業網路的管理規則，才能在有秩序的網路系統下達到企業所需的網路服務，甚至企業擁有多條對外實體線路，需要負載平衡的機制；而這些功能並不是一般 IP 分享器能夠供給的，需要更多的網路設備與 IP 分享器一同搭配才有辦法達到這個目標，但這樣的設備組合所費不貲，所以一般低價的 IP 分享器並不適用於企業對象。

新軟 Multi-Homing Gateway 不僅包含了一般 IP 分享器的功能，更具備了企業在網路管理上的需求，提供多項功能設定，將眾多的網路設備整合在一起，包含多線路負載備援、頻寬管理、防火牆、IM/P2P 管理、VPN 設定...等許多強大功能，例如公司須把 VOIP 與一般上網線路做分流並限制使用頻寬，又可能需要與分公司建立 VPN 存取之間的內部資料，這些企業大都需要使用到的功能並不是一般低價的 IP 分享器能夠提供的，另外若公司內部有大量的 PC 在使用網路，透過一般的 IP 分享器將會使的網路連線非常不穩定，而這些問題與需求只要一台新軟 Multi-Homing Gateway 便可解決，不僅所需的花費比買齊了所有功能的眾多設備還省，所占的空間更是小了許多。

企業不適用低價 IP 分享器的理由：

1. 功能性不足。
2. 無法應付多台 PC 同時上網。
3. 擴充其他設備增加所需功能需付出更多的花費，且佔用更大的空間。
4. 擴充其他設備增加所需功能，必須針對各個設備做設定非常不方便。

文 黃智傑 alex@nusoft.com.tw