新軟週報
http://www.nusoft.com.tw
Internet Security Fighter
2008/1/28-2008/2/3 第60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（二）

延續第 59 期週報『Log 的種類及功能（一）』的內容，我們將繼續介紹其他新軟系統多功能 UTM（MS 系列）及負載平衡器（MH 系列）產品內建的 Log 種類與功能：

四、IM/P2P Blocking Log：

在閱覽『IM/P2P Blocking Log』之前，網管人員必須先在管制條例（Policy）內的「IM/P2P Blocking」規則做設定。ex：網管人員在管制條例中的 IM/P2P Blocking 功能新增一條”阻擋 MSN 登入及 Edonkey 軟體禁止使用”的規則後，當使用者在使用 MSN 及 Edonkey 軟體時，不僅會發現無法登入 MSN 及使用 Edonkey 下載檔案外，同時『IM/P2P Blocking Log』也會同步記錄「哪位員工（來源電腦名稱 or IP 位址）」、「什麼時候」、使用哪套「IM/P2P 軟體」或「利用哪套 IM 軟體傳送檔案」。透過『IM/P2P Blocking Log』，可使網管人員與企業決策者清楚得知旗下員工是否在上班時間私自使用 IM/P2P 軟體的情形。

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

圖一 『IM/P2P Blocking Log』記錄內容

五、Content Blocking Log：

在檢閱『Content Blocking Log』之前，網管人員必須先在管制條例（Policy）內的「Content Blocking」規則做設定。網管人員在管制條例中的 Content Blocking 新增一條限制瀏覽網址列上含有「yahoo」字眼的所有網頁（奇摩拍賣 bid. yahoo. com、奇摩首頁 yahoo. com、奇摩新聞 news. yahoo. com. . .）及禁止所有副檔名為影像相關（mp3、mpeg、rmvb. . .）的檔案下載之管制規則。

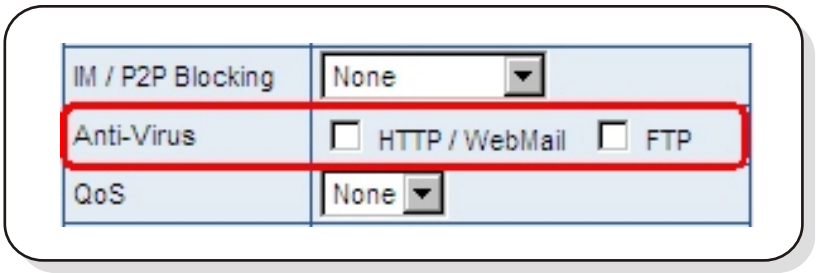
此時只要使用者瀏覽網址列上有著「yahoo」字眼的網頁，全部都將無法顯示；而使用者從 HTTP、FTP 下載影音檔案時，也將發現影音相關的檔案均無法下載。在上述情況發生的同時，『Content Blocking Log』也會同步將使用者的這些行為詳細記錄下來。透過『Content Blocking Log』，網管人員可清楚得知是「哪位員工」在「什麼時間」到「哪個地方（Web 網頁、FTP 站台...）」進行「什麼事情（瀏覽網頁、從 HTTP 或 FTP 下載檔案...）」，進而管制及掌握企業員工的網頁瀏覽與檔案下載情形。

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

圖二 『Content Blocking Log』記錄內容

六、Virus Log：（只有 NUS-MS 系列產品才有此功能）

在查看『Virus Log』之前，網管人員須先啟用管制條例（Policy）內的「Anti-Virus」規則（圖三）。當使用者透過 HTTP、Web Mail 或 FTP 下載檔案時，若下載檔案含有病毒時，系統除了會主動偵測出含有病毒的檔案名稱、類型與病毒種類，同時加以阻檔攔截其下載動作，並將資訊同步更新至『Virus Log』上。透過『Virus Log』，網管人員可得知使用者從哪些網站或伺服器下載到含有病毒的檔案，進而針對這些病毒來源網站進行封鎖管制的動作，以防檔案病毒危害到企業網路與個人資料的安全。



圖三 管制條例（Policy）內的病毒防護功能

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	Mal/Behav-053
Jan 23 12:53:06	192.168.1.28	www.asm.com	HTTP	jt.exe	Mal/Behav-156
Jan 23 12:53:06	192.168.1.24	nx.51ylb.cn	HTTP	mh2.exe	Mal/Behav-031
Jan 23 12:53:05	192.168.1.28	cn.yimg.com	HTTP	qqsg.exe	Mal/EncPk-BW
Jan 23 12:53:04	192.168.1.24	123.wwwwool.cn	HTTP	dh3.exe	Mal/PWS-N

圖四 『Virus Log』記錄內容

介紹這麼多種類的 Log，大家可以輕易的發現，新軟系統多功能 UTM（MS 系列）及負載平衡器（MH 系列）所提供的 Log，無論是資訊提供的詳細度、功能性及判讀難易都不是一般網路設備提供的 Syslog 所能望其項背的。在企業每秒必爭的網路環境上，當公司網路突然中斷、伺服器遭受不明流量攻擊或網路設備不知為何當機導致無法運作等突發狀況，網管人員如何在第一時間取得關鍵資訊來即時處理危機狀況！？此時，Log 的重要性就不言而喻了。

文 黃贊中 isaac@nusoft.com.tw

市場行銷報導 - 兩條外線可帶來什麼好處

隨著網路科技發展至今，寬頻網路的費用日漸降低，人人擁有大頻寬、高穩定的寬頻線路來架設伺服器不再只是夢想。單一線路已不能滿足現代人時常大量存取網路資源的需求，兩條外線才能提供中小企業及 SOHO 穩定的網路服務，無論是架設伺服器提供服務，或者是上網存取網路資源，透過兩條外線可讓企業網路與網際網路的傳輸更順暢。

對企業來說，兩條外線不僅能分攤企業網路的流量，也可供企業規劃網路行為的流向分配，例如規畫伺服器由第一條外線連上網際網路提供服務，一般上網行為則由第二條外線傳輸。藉由兩條外線以維持企業網路對外的服務以及其他網路行為的傳輸品質。但是，若沒有設置任何一個設備來管理企業網路與這兩條外線的運作，那麼兩條外線所能提供的功能將會遭受限制而較無彈性，在調整流量的分配上也較為不便。

新軟多功能UTM（Multi Security UTM）以及新軟負載平衡器（Multi Homing Gateway）均擁有多個 WAN Port 可支援兩條以上外線，提供「負載平衡」、「頻寬分流」、「斷線備援」等功能，將此產品設置於企業網路對外的出入口，便能統一控管企業網路對內對外的封包流向，不僅享有兩條外線的優點，並且能依照企業內部每個使用者、伺服器、網路行為等條件，分配外線使用。

使用新軟多功能 UTM 或新軟負載平衡器搭配兩條外線可帶來什麼好處：

1.負載平衡：
可將企業網路與網際網路間的傳輸流量分均分攤於兩條外線，使得網路傳輸暢通，不至於發生其中一條外線流量過大造成阻塞，而另一條外線則不常運作而造成浪費。

2.頻寬分流：
可因使用者、網路行為、服務種類...等條件，制定管理規則使該流量依循規則只通過其中的一條外線。這個功能的好處是若有需要保持某種網路服務的品質（例如 VOIP 的影音服務），那麼便可以規劃將此服務的流量與其他流量分別配置於兩條外線，如此一來該網路服務就不會因其他網路行為所造成的大流量而影響品質。

3.斷線備援：
兩條外線的好處在於當其中一條外線斷線，另外一條外線即會背負起企業網路的所有流量，維持網路的連線。假設與客戶透過網路商討會議，就算其中一條外線斷線，也能繼續維持網路會議的進行。

文 黃智傑 alex@nusoft.com.tw