新軟週報
http://www.nusoft.com.tw
Internet Security Fighter
2008/8/4- 2008/8/17 第73期

負載平衡器 / MH 系列報導

技術淺談與應用 - 監控記錄種類說明及如何妥善保存監控記錄

身為一個管理人員，除了必須控制管理公司內部所有大大小小的資訊系統、設備之外，資訊記錄的妥善保存也是相當重要的項目之一，新軟系統 MH 系列產品中【監控記錄】記錄著的各項使用者透過產品的一切操作行為資訊。這些資訊分為**流量監控**、**事件監控**、**連線記錄**、**應用程式管制記錄**、**內容管制記錄**等五大類。在這些監控記錄裡，管理者該如何才能妥善的保存所有的記錄，以做為日後公司存查的依據？這是管理人員必去須瞭解的。

流量監控：

可在設定【管制條例】時，於條例內進行設定；或在【系統管理】處勾選。而兩種設定方式的差異之處分別為，在【管制條例】中的設定時，只有設定的該項【管制條例】會詳細記錄資料封包連線。而在【系統管理】中設定時，會讓目的與來源為 MH 產品的封包皆做詳細記錄。系統管理員可在流量監控記錄裡，查詢目前進出 MH 產品各個連線狀態，包括：連線起始時間、來源位址、目的位址與處置方式等。

事件監控：

記錄產品系統組態參數值(System Configurations)更改的內容，包含更改者、更改時間、更改的參數及登入的 IP 位址…等。系統管理員可經由此事件監控功能，瞭解事件發生的時間詳細說明。

連線記錄：

記錄 MH 產品中所有的連線資訊。若連線發生問題時，系統管理員可憑藉著此資訊，進一步的了解問題的所在，以及對目前連線狀態作記錄。

應用程式管制記錄：

記錄被 MH 產品阻擋的應用程式存取資訊，系統管理員可利用此功能，立即得知應用程式的阻擋情形。

內容管制記錄：

記錄被 MH 產品所阻擋的網站存取、網頁 Script 執行、檔案下載、檔案上傳資訊，系統管理員可利用此功能，立即得知阻擋情形。

而關於記錄的備份方面，系統管理者除了可使用手動方式，隨時於系統各個監控記錄介面上點選「下載記錄」外，也可利用系統內建的監控備份功能『電子郵件監控記錄』來設定系統當記錄檔案達到特定容量時，自動發出 E-mail 提醒管理員流量監控與事件監控的記錄，或利用『遠端記錄』功能讓指定的 Syslog Server 即時接收 MH 產品的監控記錄備份，完成妥善保存以方便日後公司存查使用。

電子郵件監控記錄：

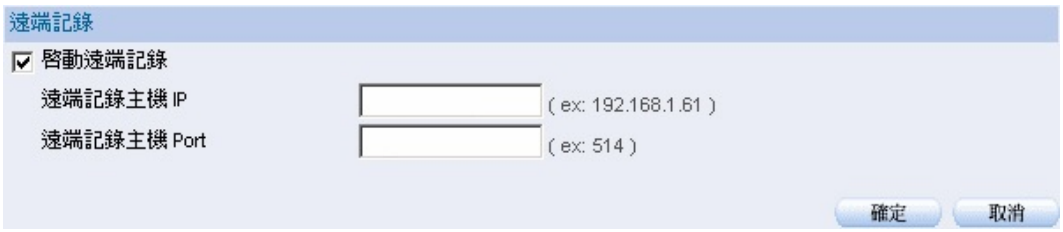
於【系統管理】→【系統設定】中，勾選【開啟電子郵件警訊通知】功能，並設定相關資料即可，完成設定後，每當監控記錄檔案到達 300 Kbytes 時，系統就會將到目前為止所累積的監控記錄，郵寄監控記錄給設定中所指定的收件者。

電子郵件監控記錄設定畫面

設定完成畫面

遠端記錄：

啟用遠端記錄功能後，可將監控記錄傳送到所指定的 Syslog Server 做備份的動作。



遠端記錄設定畫面

文 陳殿鴻 kim@nusoft.com.tw

市場行銷報導 - 3A Server的好；讓管理者感受的到

新軟系統在 MH 系列產品中使用了 3A 的功能來協助管理者能夠更輕鬆且完善、詳細的管理公司內部各種資訊系統及訊息。而 3A 則分別是 Authentication、Authorization、Accounting 的簡稱，簡單明確的讓公司內部所有使用者在經過 MH 產品做連線時，都必須經過 MH 的『認証』身份後，再經由『管制』給于授權此身份所能使用的連線權限，並且再將使用者所有的連線資訊詳細的『統計及記錄』做成監控報告，以供管理人員分析及調整各項網路政策之設定。

Authentication：產品內建認證系統，並支援外部遠端驗證撥入使用者服務(RADIUS)及 POP3 認證，多樣化的驗証設計，支援了多樣化的使用環境，管理人員可簡單的因應各種使用環境的需求。

Authorization：管理人員可利用 Policy 管制功能，搭配各項管制條例，可嚴格控管所有進出的連線，讓不同部門、不同群組、不同身份的使用者享有不同的權限，新軟系統設計的管制條例明確易懂，讓管理人員容易上手也易於控制。

Accounting：MH 系統產品提供了鉅細靡遺的連線統計報告，管理人員可依據報告內容做分析，方更將網路政策做最適當的調整，以及利用報告功能也可做最即時的線路監控。

時間	來源位址	目的位址	通訊協定	埠號	流量	處置方式
Jul 30 09:44:40	192.[illegible]	[illegible].168.[illegible]	TCP	1863 => 80	34 KB	✓
Jul 30 09:44:40	192.[illegible]	[illegible].168.[illegible]	TCP	1864 => 80	23 KB	✓
Jul 30 09:44:40	192.[illegible]	[illegible].168.[illegible]	TCP	1865 => 80	29 KB	✓
Jul 30 09:44:40	192.[illegible]	[illegible].168.[illegible]	TCP	1866 => 80	26 KB	✓
Jul 30 09:44:40	192.[illegible]	[illegible].168.[illegible]	TCP	1867 => 80	7 KB	✓
Jul 30 09:44:33	192.[illegible]	192.[illegible]	UDP	68 => 67 (WAN1)	328 B	✓

時間	管理員名稱	IP 位址	事件	內容
Jul 29 12:25:43	admin	[illegible]047	[Policy Object] Remove [IPSec Autokey] (Name : test2)	
Jul 29 12:25:41	admin	[illegible]047	[Policy Object] Remove [IPSec Autokey] (Name : test1)	
Jul 29 12:25:37	admin	[illegible]047	[Policy Object] Remove [Trunk] (Name : tt1)	
Jul 29 12:25:34	admin	[illegible]047	[Policy Object] Remove [Trunk] (Name : tt2)	
Jul 29 12:25:32	admin	[illegible]047	[Policy Object] Pause [Trunk] (Name : tt2)	

時間	事件
Jul 29 12:44:20	pluto[1256]: packet from 220.[illegible]: initial Main Mode message received on 59.[illegible] but no connection has been authorized
Jul 29 12:44:20	pluto[1256]: packet from 220.[illegible]: received Vendor ID payload [Dead Peer Detection]
Jul 29 12:44:20	pluto[1256]: packet from 220.[illegible]: ignoring Vendor ID payload [draft-ietf-ipsec-nat-t-ike-00]
Jul 29 12:44:20	pluto[1256]: packet from 220.[illegible]: ignoring Vendor ID payload [draft-ietf-ipsec-nat-t-ike-02]
Jul 29 12:44:20	pluto[1256]: packet from 220.[illegible]: received Vendor ID payload [draft-ietf-ipsec-nat-t-ike-03]
Jul 29 12:44:20	pluto[1256]: packet from 61.[illegible]: initial Main Mode message received on 59.[illegible] but no connection has been authorized

流量、事件、連線監控報告畫面截圖

除此之外還有其他多項監控報告功能，可供管理人員做更詳細的資訊控管。

在如此層層把關的環境下，不但能讓公司更有制度的運作，管理人員也只需利用 MH 的 UI 介面即可輕鬆管理所有大大小小事情，不需要像從前般的控制多台機器而手忙腳亂，當然 MH 產品的功能決不只有如此，同時還擁有 SPI 防火牆、線路即時備援、負載平衡、頻寬分流、合併頻寬的功能，也提供了完整的 VPN 解決方案（SSL VPN、IPSec / PPTP VPN、VPN Trunk），並同時具備了 IM / P2P 管制、中毒警示功能…等多項功能，一機滿足多項需求，新軟系統 MH 系列產品絕對是各公司最佳的管理產品選擇。

如需瞭解更詳細的產品資訊，歡迎至 http://www.nusoft.com.tw/

文 陳殿鴻 kim@nusoft.com.tw