新軟週報
http://www.nusoft.com.tw
Internet Security Fighter
2007/6/11 - 2007/6/17 第30期

網路記錄器 / IR 系列報導

技術淺談與應用 - Sniffer模式改良後的適用環境

新軟系統所推出的網路記錄器擁有兩種架設方式－橋接模式（Bridge Mode）與旁接模式（Sniffer Mode）。企業可依其需求選擇適用的架設方式。

當企業的網路記錄器採用旁接模式架設時，需要將網路記錄器的連接埠與 Core Switch 的鏡射埠（Mirror Port）銜接。藉由 Core Switch 會將所有經過之封包，一個不漏的複製給鏡射埠的特性，記錄企業網路往來之資訊。不用更動企業網路架構，即可完成網路記錄器的架設。

就因為網路記錄器的旁接模式架設快速、方便、隨插即用，所以有許多企業採用這種方式架設網路記錄器。但是，部分 Core Switch 的鏡射埠只有單向傳送封包之設計（只送不收）而無法雙向傳送。導致管理人員無法直接透過 Core Switch 瀏覽網路記錄器的記錄。

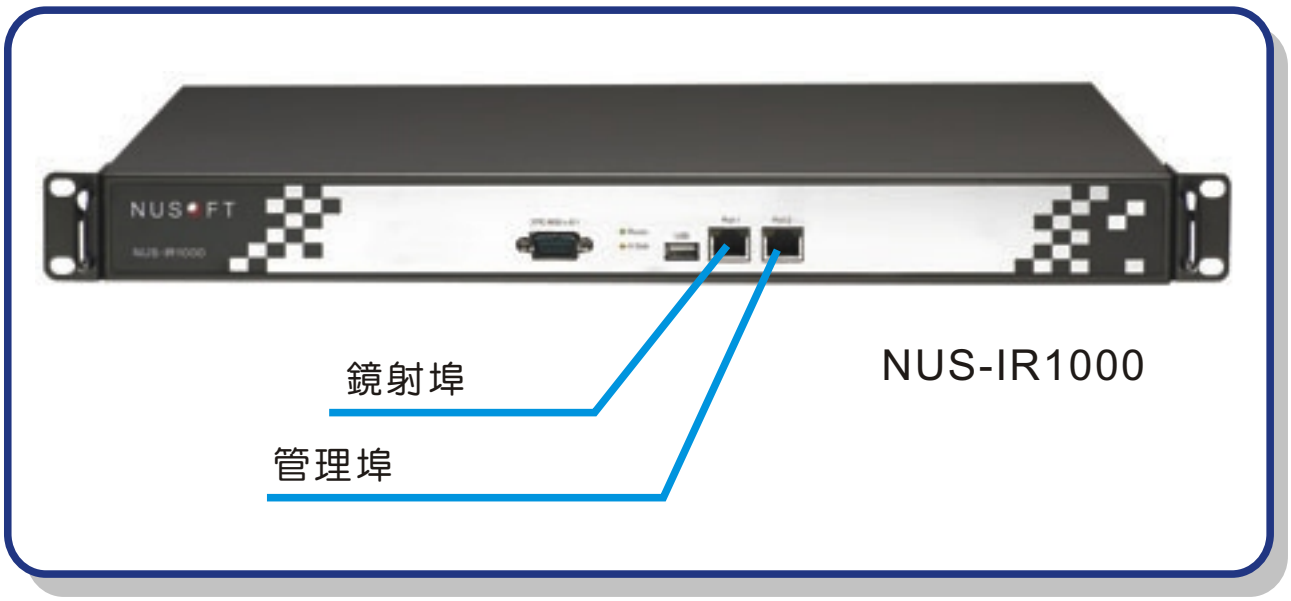
雖然絕大部分 Core Switch 的鏡射埠可定義成雙向傳送，而不會有上述的問題發生。但為了讓網路記錄器能完全適用於各種企業網路架構，因此新軟系統針對此類問題，特別增加了“網路配置模式設定”。針對這些只有單向傳送封包鏡射埠的 Core Switch 而改良。

新型的旁接模式會將網路記錄器的連接埠重新定義：

Port 1－定義為鏡射埠，專職接收 Core Switch 所傳送的企業網路資訊，而不會回應任何封包（包含 ARP）。

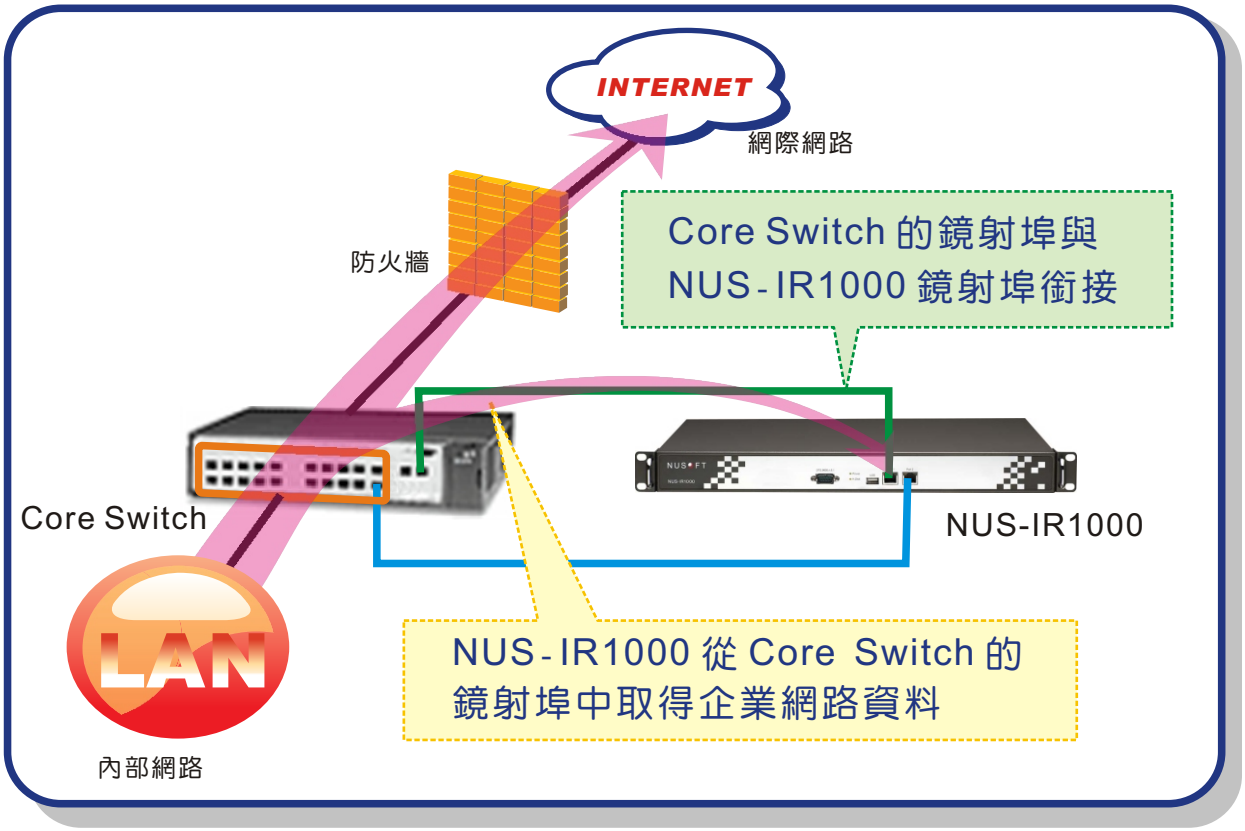
Port 2－定義為管理埠，管理人員可從此瀏覽網路記錄器之記錄。

圖一 NUS-IR2000、NUS-IR1500 旁接模式時連接埠之定義

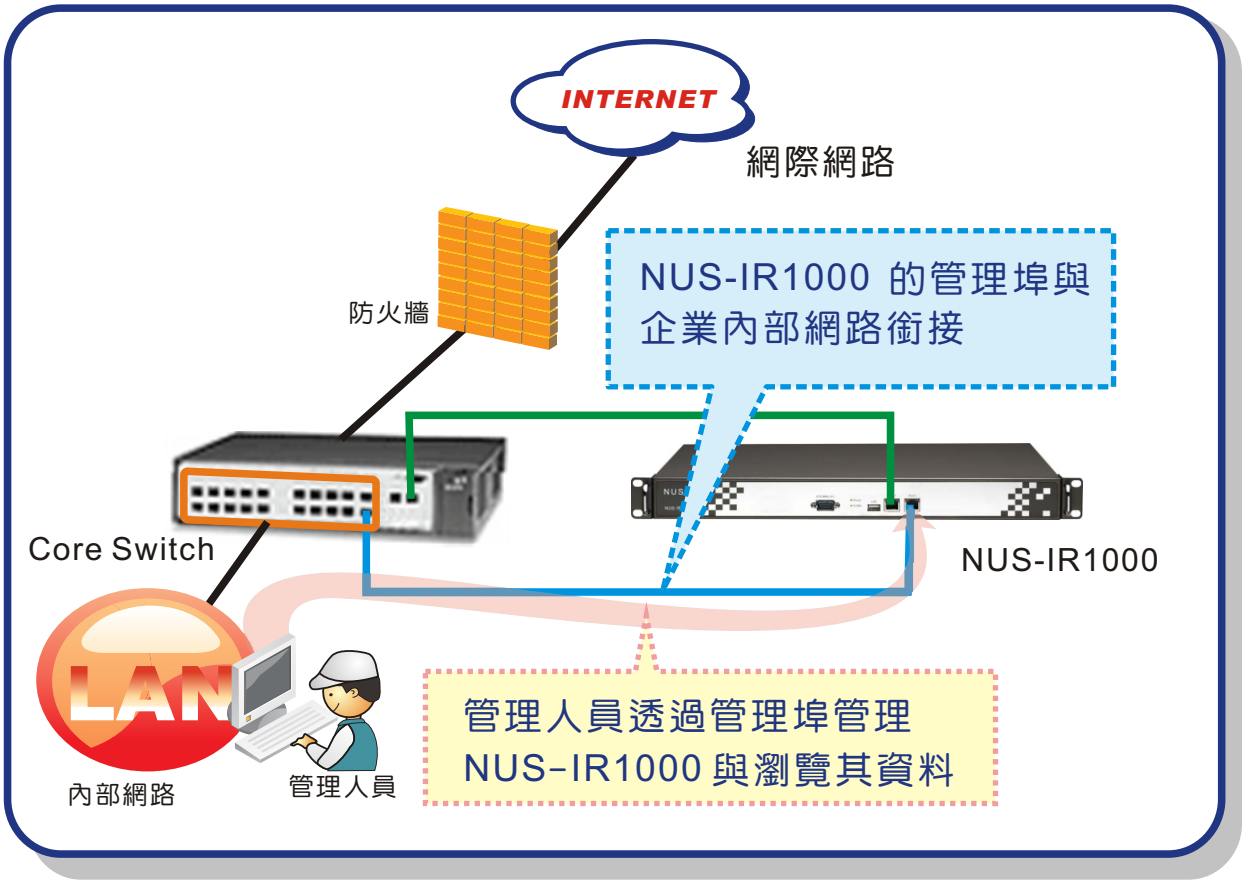


圖二 NUS-IR1000 旁接模式時接埠之定義

管理人員可將網路記錄器的鏡射埠與 Core Switch 的鏡射埠銜接，接收企業網路資訊。再將管理埠聯接至企業網路。如此一來，網路記錄器可正常記錄企業網路資訊，管理人員也可從企業網路的任何地方瀏覽網路記錄器所記錄的資料。



圖三 NUS-IR1000 利用 Core Switch 的鏡射埠取得企業網路資料



圖四 管理人員利用管理埠管理 NUS-IR1000 與瀏覽其資料

		旁接模式	橋接模式
架設方式		鏡射埠與 Core Switch 銜接。管理埠與企業網路銜接。	直接安插在企業內部網路與防火牆之間。
管理機制	異常流量偵測	僅能提出警告，無法阻擋	可提出警告，並可阻擋
	P2P 管理	無法使用	O
	IM認證/管理	無法使用	O
適用環境		當企業不想更動原有企業網路架構時適用。 必須擁有 Core Switch。	當企業需要使用網路記錄器的管理機制時適用。

表一 網路記錄器架設模式差異

文 程智偉 rayearth@nusoft.com.tw

市場行銷報導 - 全方位搜尋記錄，幫您輕鬆找到所要資料

企業e化的結果，可為企業帶來豐厚的商機。但隨之而來的員工網路摸魚、商業機密洩露...，卻嚴重損及企業之競爭力。因此，為了保護企業機密、防止員工濫用企業網路資源，國內外各家廠商紛紛推出了網路側錄相關設備，來為企業網路使用情況把關。這些廠商的網路側錄設備雖然可以詳細記錄員工上網之情況，但往往忽略掉一個關鍵重點－事後資料調閱搜尋的方便性。

要知道，在稍具規模的企業裡，網路側錄設備可記錄到的資料成千上萬，管理人員根本無從一一瀏覽查看；無法輕鬆調閱搜尋的記錄資料，對把關企業網路使用情況是無任何幫助的。因此，新軟系統在研發網路記錄器（NUS-IR2000、NUS-IR1500、NUS-IR1000）之初，就針對資料調閱、資料搜尋這部份的功能多加著墨。

新軟網路記錄器資料調閱、搜尋（以NUS-IR2000為例）

當員工透過企業網路上網時，NUS-IR2000除了會記錄其上網資料之外，其內建的分析引擎會將資料的各種特徵記錄在NUS-IR2000的資料庫中，方便管理人員日後查詢與調閱。

電子郵件（SMTP、POP3）－ NUS-IR2000除了可搜尋收件者、寄件者、主旨、時間...之外，還擁有其他廠商所沒有的**信件內容**與**附加檔案名稱搜尋**。要知道，信件內容與其附加檔案才是信件的主體。倘若無法搜尋，則在信件調閱時，容易錯失重要信件。

網頁郵件－ 一般網路側錄設備是把網頁郵件以網頁快照的方式記錄，因此系統無法判斷信件的收件者、寄件者、主旨...。在這先天不良的條件下，管理人員僅能使用URL、Web Mail Server...等無關緊要的搜尋條件調閱信件。反觀NUS-IR2000利用網頁郵件分析引擎，將網頁郵件以一般電子郵件方式記錄。所以NUS-IR2000的網頁郵件調閱搜尋方式與一般電子郵件相同，管理人員調閱起來輕鬆快速。

網頁瀏覽－ NUS-IR2000在其網頁瀏覽的搜尋介面中特別增加了**網站名稱**（URL）與**網頁內容**這兩種搜尋條件。管理人員可透過這兩種搜尋條件在龐大的網頁記錄資料中找尋所要的記錄。而用不像一般網路側錄設備，僅能透過時間這個搜尋條件來縮小記錄範圍，查閱資料相當困難。

即時通訊軟體－ 在即時通訊記錄中，最重要的當然就是員工**聊天內容**與其**傳輸之檔案**。倘若管理人員無法針對這兩個關鍵

重點搜尋，那網路側錄設備記錄在多的聊天內容也無實質作用；需要找尋的資料，很有可能是在眾多網路聊天中的一兩句話，僅用 使用者名稱、帳號、參與者...根本找不到所要資料。因此，NUS-IR2000 特別強化了這方面的搜尋功能，協助管理人員管理即時通訊軟體。

FTP 檔案傳輸－ 唯有完整的搜尋條件，管理人員方能輕鬆找到所需之資料。NUS-IR2000 的 FTP 檔案傳輸可以針對檔案名稱、FTP 主機名稱、使用者名稱、檔案大小、連線方向、時間...方式搜尋記錄，想要快速找到想要的檔案再也不是難事。

Telnet / BBS－ 在 Telnet 記錄搜尋中，Telnet 主機名稱的搜尋是重要的關鍵之一。如果想要找到員工特定的 Telnet 記錄，能從 Telnet 主機名稱的方向找尋，資料調閱將可事半功倍。

網路服務	可搜尋的特徵	
	新軟網路記錄器	一般網路側錄設備
電子郵件（SMTP、POP3）	收件者、寄件者、主旨、信件內容、使用者名稱、有無附加檔案、附加檔案名稱、信件傳送方向、時間	收件者、寄件者、主旨、使用者名稱、時間
網頁郵件	收件者、寄件者、主旨、信件內容、使用者名稱、有無附加檔案、附加檔案名稱、信件傳送方向、時間	使用者名稱、URL、Web Mail Server、時間
網頁瀏覽	網站（網站名稱、URL）、使用者名稱、網頁內容、連線方向、時間	時間
即時通訊軟體	即時通訊軟體類別、使用者名稱、帳號、參與者、內容、傳送檔案名稱、即時通訊認證帳號、時間	使用者名稱、帳號、參與者、時間
FTP 檔案傳輸	檔案名稱、FTP 主機名稱（IP）、使用者名稱、檔案大小、連線方向、時間	檔案名稱、FTP 主機 IP、使用者名稱、帳號、連線方向、時間
Telnet / BBS	使用者名稱、Telnet 主機名稱、連線方向、時間	使用者名稱、時間

表一 新軟網路記錄器與一般網路側錄設備在資料調閱、搜尋方面的差異

文 程智偉 rayearth@nusoft.com.tw