作/曹乙帆

▶ 捷宇網安總經理葉華裔表示，NetIRS是一台同時具備多功能安全機制，以及強大網管系統架構的安全控管平台，也是當前唯一敢直接進行Port Disable的安全設備。

所有網路節點及事件盡在掌握中

比SoC更強悍的NetIRS網安系統

" 捷宇網安所開發的NetIRS是一台兼具網路安全與網管特性的統合系統，提供遠比傳統SoC更具關聯性的詳盡資訊，以及精確發掘真實問題來源的能力。 "

一般人多半認為企業所面臨的安全威脅多半來自外部，但事實上依據調查指出，有8成的資訊安全威脅皆來自企業內部，Internet只佔5%而已，甚至天然災害所導致的資訊風險(15%)也比Internet高。捷宇網安總經理葉華裔特強調指出，對於企業而言，如何控管上述80%的部分才是重點。除此之外，長久以來人們一直會有無線網路不夠安全的既定想法。葉華裔不以為然的表示，無線網路在連線傳輸時多半會有加密機制的保護，反觀當前企業內部有線網路的保護機制，連無線網路的都不如，如此更加突顯出企業內部網路安全需要再提升的迫切性及重要性。

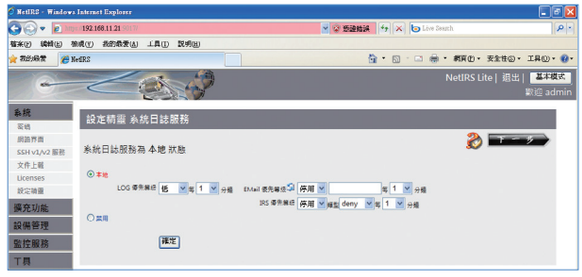
面對網路安全問題，傳統SIEM/SoC只會分析出某個IP有問題，但卻無法確知IP背後的真實身分是誰，同時更別提IP盜用該如何因應了。不僅如此，SIEM/SoC針對特定事件多半只提供建議，而不會主動解決問題。換言之，企業管理人員仍需「徒手」面對可能的安全威脅，如此一來，不但增加管理負擔，也可能緩不濟急。

結合網管系統架構的捷宇網安NetIRS系統，堪稱是進階多功版的SIEM/SoC，該系統不但整合了當前多種主流網路安全機制，同時支援主機監測、階層式流量地圖、流量分析、資安事件收集分析告警、和即時入侵反應系統(IRS—Intrusion Response System)等功能。再加上線路分析機制的加持，因而可以鉅細靡遺地偵測收集到企業內部所有網路資源及資訊，進而掌握網路所有狀況，並精準確認出問題來源，接著在第一時間內加以封鎖。

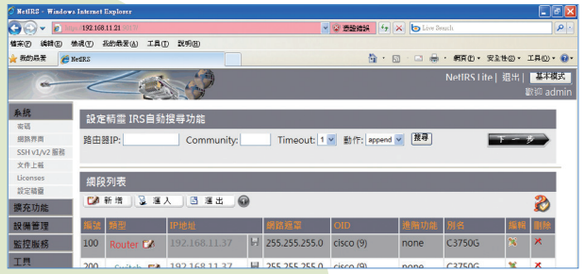
強大多功也能在精靈導引下輕鬆完成設定

雖然NetIRS是一台支援多功能網安及強大網管功能的全方位SoC平台，但設定上一點都不難。使用者只要隨著設定精靈的指示及導引，便可完成整個系統的初始設定作業。

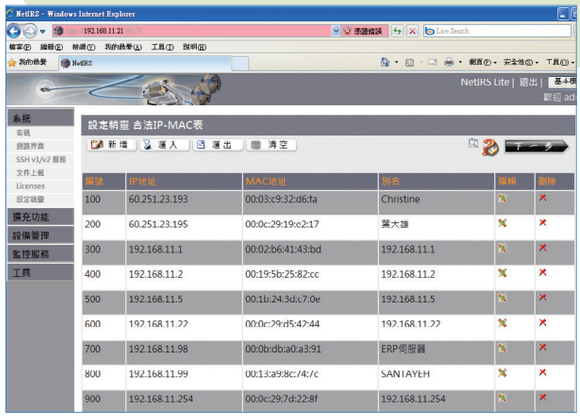
▶ 透過設定精靈，在一般網路環境下，只需10分鐘就可以將畫面所示步驟中的所有功能設定完成。



▶ 本此頁面下可設定syslog的搜尋作業，以及相關對應動作的設定。



▶ 接下來要設定到底要管多少網路設備，在此會透過IRS自動搜尋功能將設備一一列舉，大約一個Class C下的設備會在6秒鐘搜尋完成。找完後，會自動列出設備名稱及廠牌等資訊。

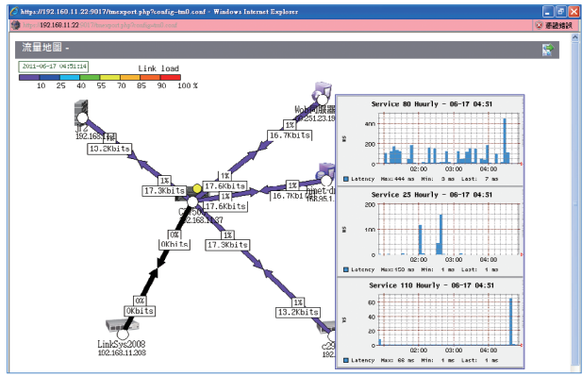


▶ 本頁面可進行使用者控管設定，而且別名也可以是中文，方便管理者檢視。例如哪一個使用者用什麼IP、配什麼Mac地址，皆可在此檢視並管控，以確保使用者有沒有盜用別人IP的情形。

▶ NetIRS設備有提供DHCP服務，藉此可以提供IP Mac控管、MAC認證、網頁認證等特定功能。

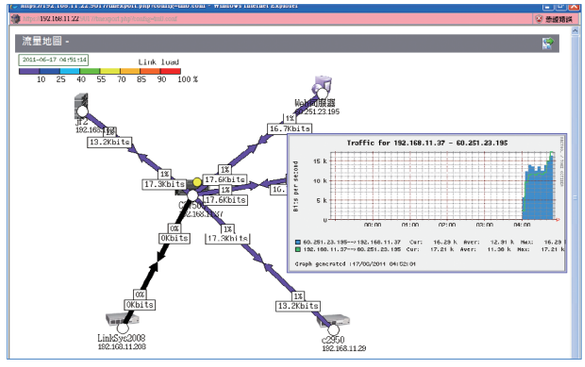
▶ NetIRS設備也支援伺服器監控，例如，只要加進監控伺服器之特定服務，便可針對某台伺服器上的特定服務加以監控。

▶ NetIRS最令人稱道的功能莫過於線路分析功能，該功能可以找出設備之間到底是如何界接在一起。只要在本頁面中點選確定採取Auto Configruation，該精靈會自動完成線路分析設定。



▶ 在流量地圖中，可以看到設備的狀態。而且使用者可將滑鼠移到圖上不同地方，會分別秀出詳細的資訊，幫助管理人員掌握各種狀況。如圖所示，將滑鼠移到Web Server上會秀出該伺服器的服務狀態。

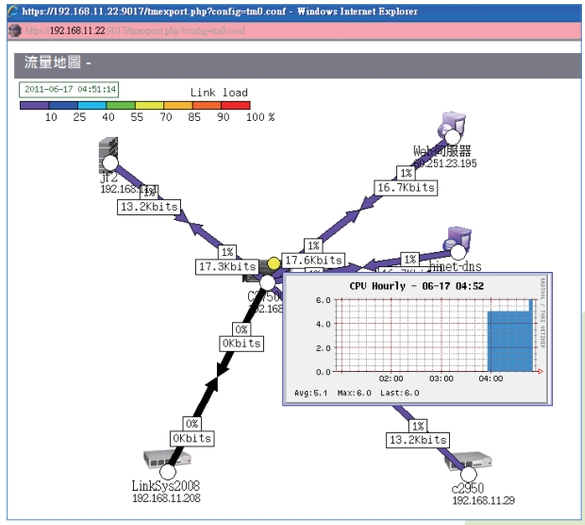
▶ 點取下一步後，頁面會秀出所找到的設備詳細資訊，同時右上角會秀出設備連結狀況的流量地圖。



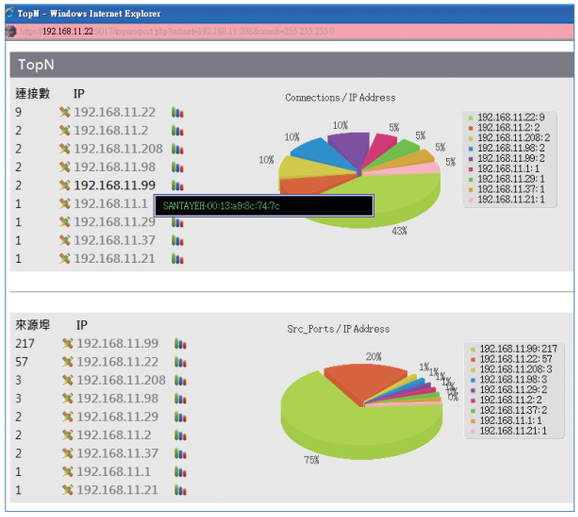
▶ 使用者可以點選不同線路，進而監控不同線路的流量狀態。

一目瞭然地掌握所有關聯訊息的流量地圖

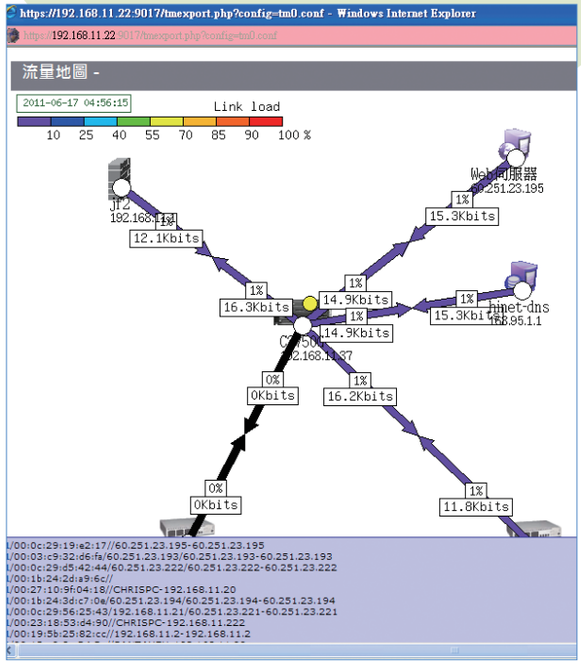
透過日誌搜尋、進階線路分析及主機監控機制，再輔以強大的資源資訊關聯能力，NetIRS設備可進一步將企業現有整體架構，繪製成一目瞭然的流量拓璞圖。針對不同企業規模，其最高可支援36張流量地圖，所以即使再大規模的企業網路架構，都可以多張流量地圖完整呈現。由於具備強大關聯能力，所以圖上的每一節點、每一線路，都可藉由滑鼠點取秀出更豐富的資訊，堪稱是安全管理上的一大利器。



▶ 流量地圖中黃色圓圈表示該設備的CPU資源耗用狀況，使用者可針對特定交換器，進行CPU、記憶體等資源使用率狀況的監控。一旦該資源超過設定值，便會出現紅圈。此外，圖中黑色線路表斷線狀態。

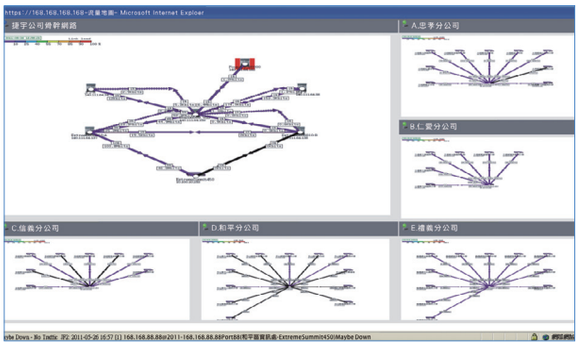


▶ 使用者可以點取某個節點，接著會立即分析出流量狀況，同時依據不同IP列出流量TopN排行結果。不僅如此，NetIRS並具備自動關聯能力，當管理人員將滑鼠游標移到相關IP上，便會立即秀出相關資訊，管理者立即可知該IP使用者姓甚名誰。

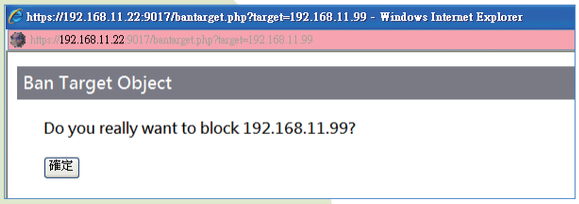


▶ 將滑鼠移到交換器的某個埠上，便可立即清楚看到目前有多少使用者正連上這台交換器上。同時，接到哪個埠？用什麼IP、MAC及Admin等資訊皆可一目瞭然。

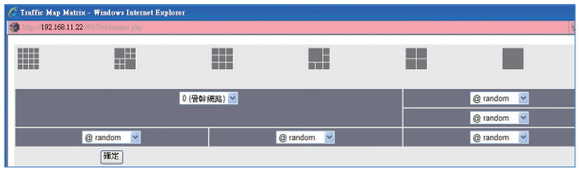
▶ 若想更進一步知道某使用者到底在跟哪些人連線的話，只要點取該IP，便會跳出相關資訊的詳細頁面，管理者可以藉此掌握使用者是否有異常的行為。



▶ 對規模較大的企業而言，整個公司設備架構可能無法用1張流量地圖來呈現。NetIRS流量地圖不但最多可支援36張流量地圖，同時支援多宮格畫面顯示功能。如果企業流量地圖很多，無法在6宮格中一次秀出，便會以輪播的方式切換顯示。



▶ 如圖所示，一旦發現使用者有任何異常的狀況時，可以點取確定鍵加以阻斷。



▶ NetIRS設備在流量地圖製作上提供不同Layout的宮格排列樣式，在多宮格顯示上，該設備支援多種排列組合，並可指定特定宮格要放哪張圖。同時針對不同螢幕，還會自動調配每個宮格中的螢幕解析度。