眾至資安三劍客 內網防護解決方案

現代人每天的生活都跟網路息息相關，用網路看新聞、聽音樂、找資料等，大至政府單位小至公司行號，因此資料的安全性就顯得格外重要。那為何即使大家都有這樣的認知，也安裝了防火牆用來過濾、阻擋惡意來源，資安事件卻還是頻傳呢？
其實很簡單，原因在於內網的流量防火牆並無法阻擋，其流量是橫向而非縱向，所以當然不在防火牆的管轄範圍內。

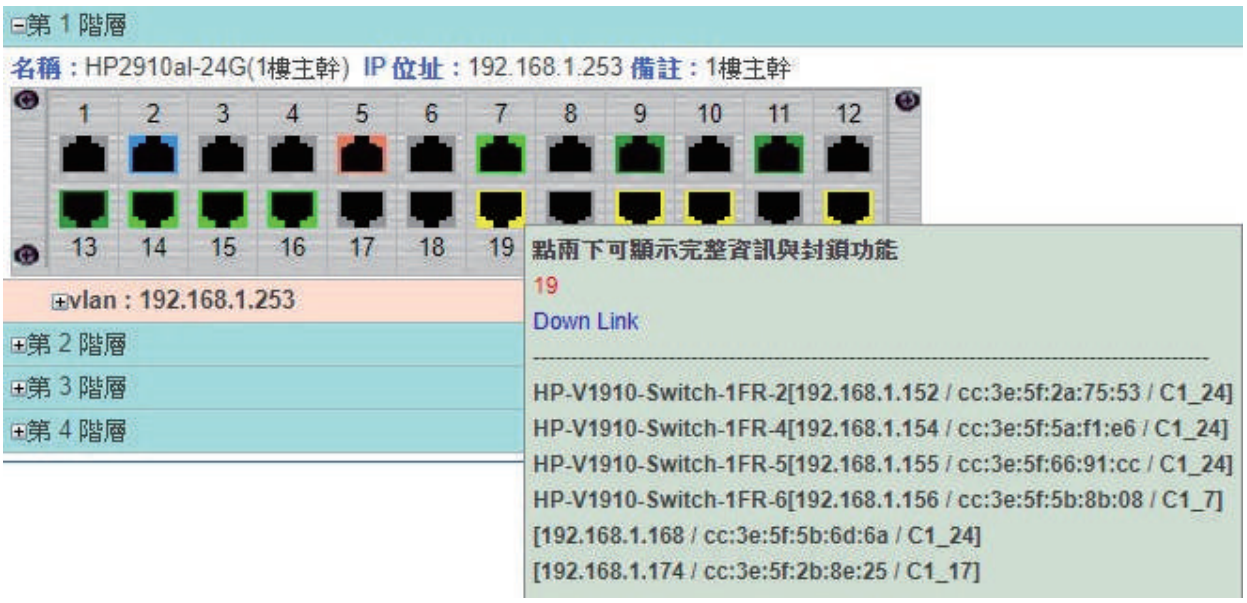
那為何內部會發生問題呢？舉例如下：
1.行動裝置：平常上網不受防火牆管控，到公司後變成WiFi上網，進而感染內網。
2.隨身碟：從外部攜帶進入公司，接入電腦，導致內部感染。
3.一般上網：員工內部電腦下載檔案後，該檔案尚未被觸發，因而沒被防火牆偵測到。
4.除了上述情況，若有經過防火牆的也會被阻擋，但僅僅是不能上網，還是會影響到內部群組。

為因應這些情況，眾至特別推出「資安三劍客」之解決方案，透過整合交換器及AP，將L2層級的資訊整合至防火牆上，就可以確認交換器上每個Port的流量、連線的成員以及網路的階層拓樸圖等；AP部份不僅可以看到無線的使用者，還能當作AP控制器，統一派送SSID、密碼等資料，無須個別登入每台AP去做設定，加上搭配防火牆異常流量、IPS機制，當異常發生時，除了在防火牆上的封鎖之外，再結合交換器直接封閉來源網路孔，避免有問題的裝置持續在內網擴散。
以下分成三個機制來詳解「資安三劍客」：

台中總公司 04-2705-0888
台中市西屯區西屯路二段256巷6號3F-6
台北分公司 02-2501-1185
台北市中山區松江路129號6F-2
高雄分公司 07-229-8788
高雄市新興區民權一路251號8F-6
免付費專線 0800-666-188
官方網站 | www.sharetech.com.tw
銷售諮詢 | sales@sharetech.com.tw
技術支援 | help@sharetech.com.tw

交換器管理

與交換器綁定後，即可確認交換器各個網路孔的狀態和網路孔上的成員，且防火牆會根據所收集到的資訊，將設備階層排序；介面上的網路孔也會依據當前狀態顯示不同的圖示，比如：有通電但沒封包，藉由簡單明瞭的圖示讓網管人員一目了然。如下圖一所示：



圖一：交換器階層圖

AP管理

AP整合後，防火牆就可以當作AP控制器，統一派送SSID名稱、密碼等資訊。設定畫面上還能確認每個AP是否正常及成員人數等，如此一來，不管是有線或無線上網都一清二楚。如下圖二所示：

圖二：AP管理

內網防護

整合AP與交換器後，當有流量（如異常的流量與Session、IPS）觸發防火牆的條件時，防火牆會主動通知交換器並關閉異常的網路孔，將災害封鎖至最小，不讓問題設備持續在內網擴散造成更嚴重的危害。如下圖三-四所示：

限支援協同防禦的交換器型號

圖三：異常流量阻擋條件設定

圖四：針對偽造的IP/MAC，與IPS連動封鎖

※詳細資訊請參考手冊