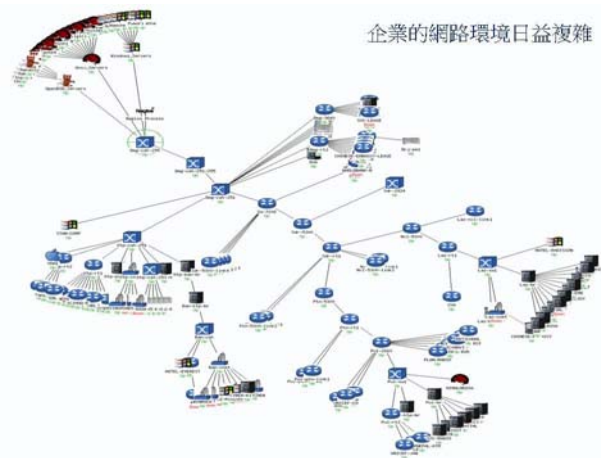


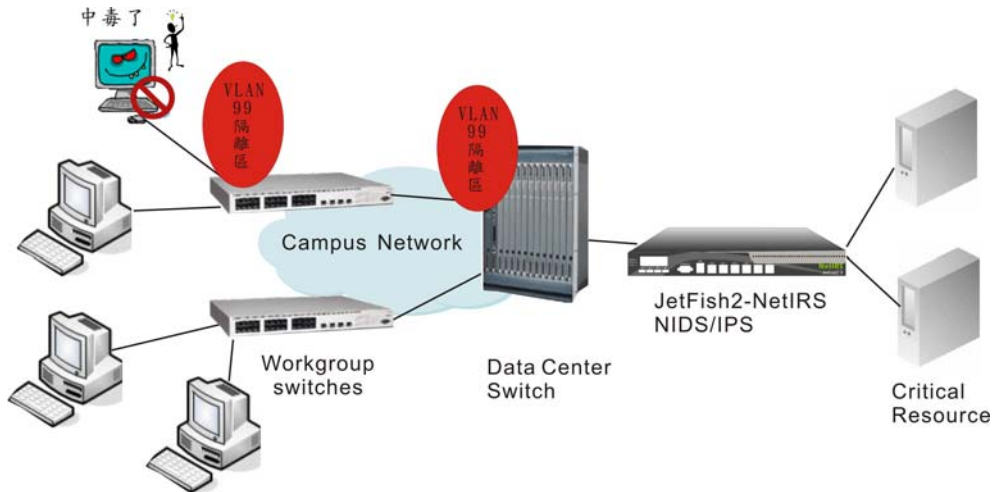
漫談內網資安管理(二)

作者: 葉華裔
捷宇網安股份有限公司 總經理
E-Mail: santayeh@netaxle.com.tw

了解自己，了解你的敵人

網路管理人員常常著重於尋找高效能的防火牆、入侵偵測系統或防毒牆為企業網路對外來的入侵建立起一道嚴密的防線保護網路的安全，然而企業內部的安全控管卻不受重視。其實最大的威脅有可能潛藏於企業內部使用者或連結於企業網路的各種電腦設備，因為企業資訊安全威脅有 80% 來自內部。有關內部網路資安管理，筆者在上期文章中提及網路攻防的重點在 — 時間。時間效率決定了網路是否被攻擊癱瘓或者防禦成功，然而攻防的背後還隱藏了另一個重要因素 — 人(或者說是網路節點)。雖說企業資訊安全威脅有 80% 來自內部，但當更進一步分析這 80% 資訊安全威脅時，可發現其中有 40% 根本是來自非授權使用者的不當行為，非授權使用者可能為企業的訪客、臨時或外聘的工作人員、甚至是開放空間的所有人如校園、醫院、政府機關等等。會影起非授權使用者對內部網路造成傷害的部份原因，可歸咎於傳統的網路觀念與網路佈建方式，在大部份的有線網路環境中，使用者只要捉到一條網路線接上筆記型電腦，網路大概就通了，最多只是不知 IP 該如何設定，若是企業內部環境有提供 DHCP 服務時，還會自動分配給非授權使用者一組 IP；若非授權使用者真的需要一個 IP，其實只要使用 Sniffer 軟體分析一下封包便也不難猜出企業 IP 的設定，然而對一個惡意使用者或攻擊者而言，有時連 IP 設定都不需知道就可破壞與攻擊網路了。而要防止非授權使用者的攻擊同時不影響其他人的操作，找出這個攻擊者就成為首要要務。





上圖: NetAxle 公司的 NetIRS 可以在複雜環境中鎖定攻擊者並將之隔離。

就算對於真正善良合法的使用者 (或節點) 而言，了解其在企業內部網路上的真實身份也是非常重要的。某些行為在使用者身上是異常行為，但在伺服器上可能是正常的；相對的，某些行為在伺服器上是異常行為，但在使用者上卻是正常的。所以要防範合法的使用者因未知而導致的不當行為或人為疏失（如無意間散播了病毒等…）傷害了內部網路（因內部授權者的不當行為或人為疏失而造成內網威脅佔了另外的 40%），是故了解每個節點的身份在網路攻防策略中佔了非常重要的地位。

使用者管控萬靈丹

然而隨著網路的發達與普及，不同的使用者管控應用型態混雜在同一公司中，固定 IP 與 DHCP 環境，固定式桌上型電腦與移動式筆記型電腦，都牽扯到管控機制是否符合公司應用環境與需求。簡單來講，沒有單一一種管控機制可以符合企業多型態的應用需求。傳統上使用者管控機制分為 IP-MAC 鎖定與 DHCP，兩者各有優缺點，管理者可視網路環境需求選擇。然而現階段最常遇到的問題是——現在的網路同時需要兩種以上的管控機制。例如 IP-MAC 鎖定是較為安全的管控機制，一個 MAC 地址固定分配一個 IP 地址，若一個企業有 200 個使用者節點，就需管理 200 個 IP-MAC 配對；但若這 200 個使用者有移動的需求，會在企業內各網段活動或到會議室開會使用網路，管理就會變得複

The screenshot shows a network management interface with a table of IP-MAC bindings and a configuration panel for IP-MAC binding and ARP locking.

ID	IP	MAC	Static	Bind	Port
100	192.168.10.11	0800a0c8101010	Y	Y	1
200	192.168.11.30	0800a0c8113333	N	Y	1
300	192.168.11.99	a98c747c	Y	Y	1
400	192.168.12.12	0800a0c8121212	Y	Y	1

The configuration panel shows the following settings:

- IP-MAC 鎖定: 啟用 IP-MAC 鎖定? (Enabled)
- IP MAC Binding ARP Locking: Add 192.168.10.11 0080c8101010 into switches. Add 192.168.11.33 0080c8113333 into switches. Add 192.168.11.99 0013a98c747c into switches. Add 192.168.11.213 000c2999ae27 into switches. Add 192.168.12.12 0080c8121212 into switches. Finished.

ARP 自動寫入 Layer3 Switch

雜；若此企業有 10 個網段，那管理的 IP-MAC 配對就變成 $200 * 10 = 2000$ 個，後續的管理維護變得更為困難。相對的，在有移動需求的網路環境中使用 DHCP 做為使用者 IP 管理機制就較為方便，然而傳統 DHCP 服務又有其安全考量，並且不是所有節點都可或適合使用 DHCP。

傳統 DHCP 服務器的運作方式是當有使用者發出 DHCP 請求時，若伺服器有空 IP 即會配發 IP 給使用者，不論使用者是否為合法使用者 (DHCP 服務器也無法判斷是否為合法使用者)，因此造成很大的網路安全漏洞。在較新型的 DHCP 服務器中可提供 MAC Authenticated DHCP Service，DHCP 服務器在分配 IP 前會先確認使用者的 MAC 地址是否是一個合法使用者，若是，才分配 IP；如此就可在 DHCP 環境中，依然提供較安全的防護。

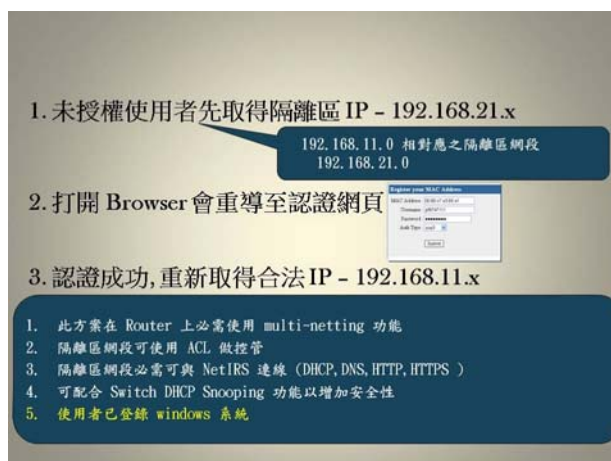
在許多的情況下，管理者會希望針對不同的節點特性與需求，同時使用 IP-MAC 鎖定與 MAC Authenticated DHCP 服務。但無論是何種機制，事前的調查動作都是必要的程序，確認所有合法節點的 MAC 地址，若使用

IP-MAC 鎖定則再加 IP 地址。然而企業內若網段與節點數不少，這對管理人員是很吃重的工作，光是確認合法節點的 MAC 地址就得耗費不少心力，諒論那些變動頻繁的部門。因此若能有一種不需事前登錄節點 MAC 地址且依然可確認使用者為合法使用者再授權其使用網路的機制，對管理者而言可減輕不少負擔。常常使用在無線網路的 Web Portal 認證機制就是此種機制之一，使用者利用無線上網時，Web 會先跳出認證網頁，使用者在輸入帳號密碼並檢驗成功後即可取得網路使用權。同樣的原理也可應用在有線網路中。



Web Portal 認證機制最重要的關鍵在於是否可整合現有使用者帳號密碼資料庫，可能為 AD、LDAP、RADIUS TACACS+、email 等，因為使用者都不希望為了認證機制而必需多管理一個帳號。

但 Web Portal 在 AD Domain 環境下會有點小小不方便之處，因



為使用者在 AD Domain 的環境中當開啓 windows 時已經要求登錄 AD Domain 一次，使用者此時已經輸入帳號密碼，但在進入 windows 後還需再開啓 IE 使用 Web Portal 登錄一次，此時還需再輸入一次 AD 帳號密碼，那對使用者而言其實是已經輸入兩次帳號密碼了。所以在整合 AD 的環境中最好支援 Single Sign-On 的功能，也就是當系統偵測到使用者已成功登錄 AD Domain 後就直接授與網路使用權，而不需再經 Web Portal 的認證。



使用者認證與管控的另一個好處在於其詳細的報表

網域使用者 (總和 23)						
IP地址	MAC地址	使用者帳號	NetBIOS 名稱	NetBIOS 群組	開始使用時間	最後使用時間
192.168.110.51	00:24:1d:73:d4:6e	labtest	98296	NETAXLE	2010-09-06 08:08:31	2010-09-09 08:53:06
192.168.110.58	00:24:1d:75:45:7b	qwer	98259	WORKGROUP	2010-09-06 08:38:23	2010-09-09 08:34:05
192.168.110.59	00:24:1d:74:a8:91	santa	98290	WORKGROUP	2010-09-06 08:13:40	2010-09-09 08:39:18
192.168.110.60	00:24:1d:74:0c:c5	office	98291	WORKGROUP	2010-09-06 08:13:33	2010-09-09 08:39:28
192.168.110.61	00:24:1d:73:d0:c6	office	98297	WORKGROUP	2010-09-06 08:28:57	2010-09-09 08:16:33
192.168.110.62	00:24:1d:75:0d:d8	office	98295	HKS	2010-09-07 07:55:03	2010-09-09 07:44:49
192.168.110.63	00:24:1d:75:10:bc	office	98288	NETAXLE	2010-09-06 08:05:22	2010-09-08 08:13:18
192.168.110.66	00:24:1d:74:18:82	office	98292	WORKGROUP	2010-09-06 08:08:26	2010-09-09 08:52:14
192.168.110.68	00:24:1d:74:10:52	office	98293	WORKGROUP	2010-09-06 08:11:01	2010-09-09 08:48:10
192.168.110.69	00:24:1d:74:a8:6e	office	98286	WORKGROUP	2010-09-06 08:08:52	2010-09-09 08:39:16
192.168.110.70	00:24:1d:73:b6:19	office	98285	WORKGROUP	2010-09-06 08:08:42	2010-09-09 08:38:49
192.168.110.71	00:24:1d:73:ff:0b	office	98287	HKS	2010-09-06 08:08:46	2010-09-09 08:41:18
192.168.110.98	00:50:ba:bc:5e:2ec	methad	96196	NETAXLE	2010-09-06 10:37:19	2010-09-08 11:24:11
192.168.110.101	00:11:d8:83:bd:4b	office	94266	HKS	2010-09-08 03:13:29	2010-09-09 03:13:07
192.168.110.140	00:1e:4f:7e:54:b	office	97102	NETAXLE	2010-09-06 08:30:46	2010-09-09 08:16:28

時間標記	事件	來源	目的地址	狀態
2010-09-08 17:45:01	192.168.11.213 Interface 3(Web-UI - qazsw) Traffic Overload 0Mb(54%) - 0Mb (100%)	192.168.11.213@3:0	0.0.0.0	🇩🇵🇮🇹
2010-09-08 17:00:01	192.168.11.213 Interface 3(Web-UI - qazsw) Traffic Overload 0Mb(20%) - 0Mb (91%)	192.168.11.213@3:0	0.0.0.0	🇩🇵🇮🇹

從報表可以清楚的知道有多少使用者登錄到 AD Domain，有多少的 windows 使用者，有多少 IPv4/IPv6 節點與相關資訊。如此不僅方便查詢使用者使用資訊做為資安事件追蹤依據，也可為將來個資法實施時事先鋪路。

彈性是成功的要件

然而應用在實際環境上出現了許多的困難，複雜的異質網路環境是導入使用者管控機制面臨的最大難題。不像防火牆、入侵偵測系統等設備是獨立運作，使用者管控機制牽涉到相關的網路設備 (Router, Switch 等)，網路架構，各種不同廠牌和組態的端點設備，與使用者帳密資料庫的結合；而且還需考量不斷演進的新型應用與設備 (如 iphone 與 ipad) 的出現是否會受到限制。



上圖: 即便 User 使用 iphone 或 ipad, NetIRS 提供有線與無線網路認證模式, 支援 windows SSO 應用, 並整合 AD Domain 達成一次性簽入。

因此管控機制的彈性是成功最重要與唯一的要件。雖然科技終有其限制, 但科技的目的是為了解決問題並減輕管理人員負擔, 而不是使人綁手綁腳。傳統的使用者控管機都只提供單一功能, 因此常會看到一個企業在無線網路使用一套系統與管控機制, 有線網路使用另一套系統與管控機制, 會議室又是另一套系統與管控機制, 不僅耗費了許多成本, 在管理維護與員工使用上更是增加許多不便, 當有資安事件發生時, 管理者還需查詢三套資料庫找出有問題的使用者。

若一個系統能提供不同控管機制且能同時並存與混合使用, 並且使用同一個資料庫儲存使用者使用記錄, 對現在多變的網路環境才是最佳的解決之道。