

## 內網安全新境界(二)

---

### 淺談 NAC 解決方案的發展

#### 前言

很多 IT 管理人員及主管，時常抱怨已經花了大把的鈔票在端點資安的建置及維護，但是效果看起來還是有限，譬如：所有的電腦都已經裝防毒軟體，會什麼還是有員工會遭受已知病毒的感染？或者 IT 採購的個人防火牆及防毒或防駭軟體，各個單位的使用者到底有沒有安裝？安裝了有沒有啟動？有沒有更新到最新版的病毒碼？除了這些之外，電腦裏面安全性層級的設定為何？因為 IE 及 MS Office 也是容易遭入侵的漏洞，這些都是大部份管理者想要知道答案的問題！

另外，對於 VPN 的用戶、來賓(Guest)或者協力廠商等，使用的電腦非受 IT 所管控，但這些人員對於內網的威脅跟內部的電腦無異，所以更需要進一步檢驗是否符合基本的安全設定要求，才准許使用內部網路資源。

#### NAC (Network Access Control)

為了解決上述的一連串問題，在幾年前就已經有廠商發標所謂的網路存取控(NAC)的解決方案，透過 NAC，管理者可以針對不同群組的使用者的電腦進行檢驗，檢驗的項目包含，各種作業系統的 Service Pack 及 Hot Fix 是否已經更新，各種防毒、防火牆、Anti-Spyware 軟體是否已經安裝、啟動以及更新到最新的特徵碼，IE 及 MS Office 軟體的安全性設定是否符合規定，有無安裝禁止使用的軟體，規定要使用的軟體是否安裝....等，它的功能雖然強大，是內網安全性政策監控及規範不可或缺的工具，但直至今日，大部份的廠商的解決方案還是普遍性的存在下面幾個問題。

- 1). 必須透過特定的網路架構或搭配特定的功能。

- 2). 必須要安裝用戶端軟體且只支援特定的作業系統。
- 3). 檢驗的項目不夠或者檢驗的時間過久。
- 4). 無法進行持續性的檢查。

## 問題 1：必須透過特定的網路架構或搭配特定的功能

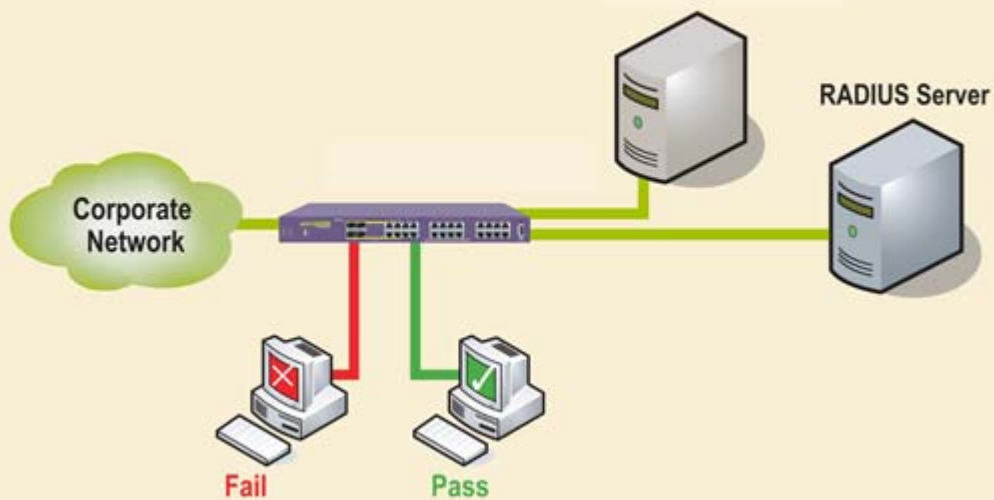
要讓每個用戶接受檢驗，必須要具備一個強制性的環境或架構才行，其中最簡單的莫過於閘道型的網路架構，將具備 NAC 功能的設備置於用戶必經的路徑上，此時用戶只需開啟瀏覽器下載 ActiveX 即可，這也是市面上的 VPN 設備常見使用的方法，如果用戶拒絕下載 ActiveX 接受檢驗或檢驗不通過，那麼 NAC 的設備就可以禁止該用戶存取內部網路。

但是可想而知，這樣的架構在著重效能的內網並不適用，因此 NAC 必須要搭配其它的方法才行，其中最常見的是搭配 802.1x，因為使用者必須經過 802.1x 的認證才能使用網路，NAC 便可利用使用者登入網路時進行檢驗的動作，這樣的架構對 NAC 來講沒有任何問題，但是對管理者而言 802.1x 本身卻是一大挑戰。

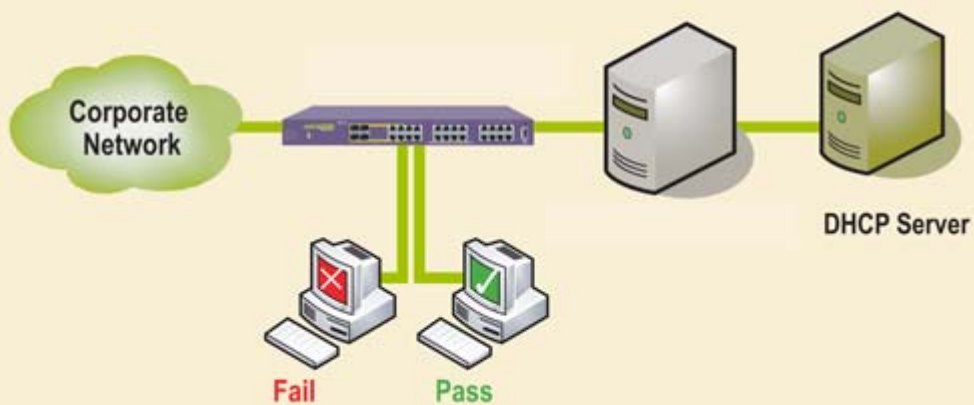
原因在於要啟用 802.1x 必須要多方面的配合，其中最困難的是 802.1x 必須要搭配網路交換器的能力，如果交換器沒有支援針對每個用戶作認證，而是針對每個介面做認證的話(802.1x 標準是 port-based 認證機制)，那麼所有連接使用者的網路交換器都必須要汰換成支援 802.1x 的交換器，但如果網路交換器可採取對每個用戶進行認證的話，當然只要收容層(Aggregation)的群組交換器支援 802.1x 即可，另外一個大問題在於，使用者的電腦也必須支援 802.1x 的用戶端軟體才行，更別談還要採用認證伺服器或憑證的等鎖碎的工作。

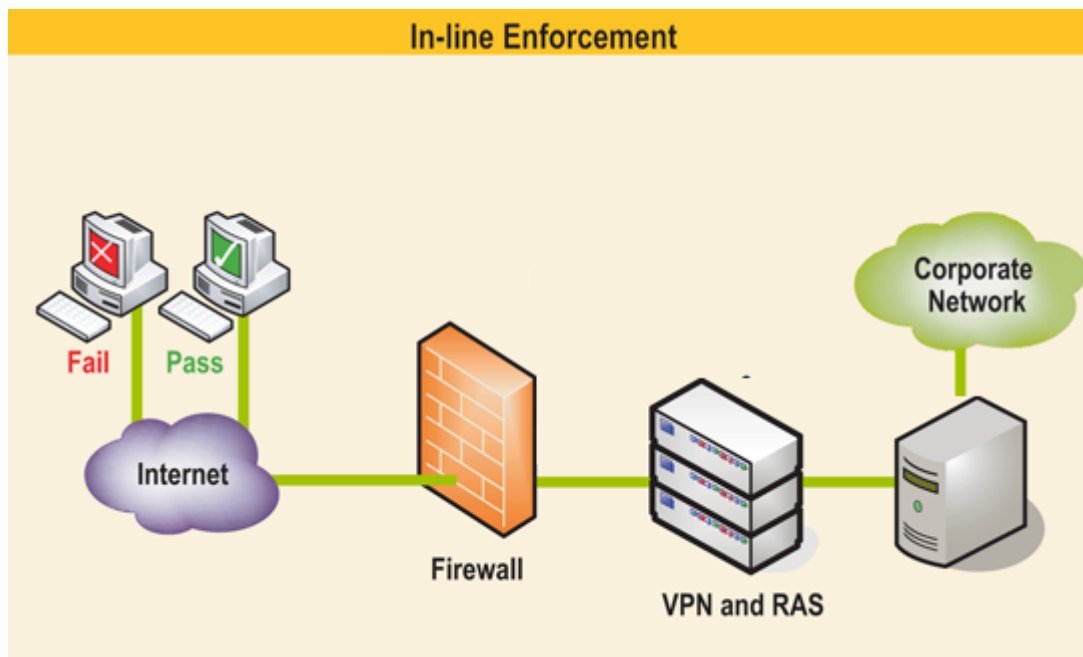
許多廠家為了避免 802.1x 使用的困擾，造成 NAC 無法使用的困境，紛紛支援 DHCP 的架構，它使用的道理也是非常簡單，將 NAC 的設備架設在 DHCP 伺服器前，NAC 就會在使用者取得動態 IP 前進行檢驗的動作，這樣的架構之所以可行，原因在於現有的網路交換器大都支援所謂的 DHCP Snooping 有關，透過 DHCP Snooping 功能的啟動，使用者就無法使用自訂 IP 或擅改 DHCP 發放的 IP，因此使用者非啟動 DHCP 的功能不可，使用這種架構的好處在於只要 Layer 3 的設備支援這樣的功能即可，網路架構或設備不需做大規模的更動或更新。

### 802.1x Enforcement



### DHCP Enforcement (Network & Endpoint based)





## 問題 2：必須要安裝用戶端軟體

由於 NAC 必須檢驗用戶的電腦，因此在用戶端安裝軟體是最有效的方法，但是這會延伸出兩個問題，第一是用戶端的軟體只支援特定的作業系統，目前 NAC 的解決方案絕大部份只適用於 Windows 作業系統，對於 Mac 或 Linux 平台的支援較少，廠商的回應大都是因為這些作業系統中毒的機會相對性的較低，但問題是這些工作站通常有特定的重要用途，也是不得受到監控的對象之，第二是用戶端軟體的維護相對的增加管理人員的負擔，使用者無意的移除軟體，可能讓管理人員疲於奔命。

除了於安裝用戶端軟體外，最新的趨勢是使用所謂的 Agentless 的作法，當然這也需要一些條件的配合，譬如搭配 MS AD 或者要求使用者於第一次使用 NAC 時連結至 NAC 設備輸入本機的管理者密碼即可，這樣就可以採用不安裝用戶端軟體的檢驗方法。

## 問題 3：檢驗的項目不夠或者檢驗的時間過久

NAC 另一個問題是，檢驗的項目不夠或者不夠深入，除了一般的測試項目之外，某些單位可能會需要檢驗使用者是否安裝一些客制化的軟體，例如：資產管理軟體、硬體檢測軟體...等進行檢驗，但是如果檢測的項目過多，可能會造成檢驗時間過久的狀況，另外不同的檢測方式，如安裝用戶端軟體、Agentless 及 ActiveX

檢測的項目也有可能會有不同的狀況，這些都是管理人員在導入 NAC 時必須要注意的問題，一般而言，使用者對於檢測時間的容忍程度大約在 15 秒到 30 秒之間，一旦超過這個時間範圍，使用者大都會覺得不耐煩，這將會影響使用者的觀感及接受程度，更何況於上班尖峰時間可能會有更長的等待時間！

#### 問題 4：無法進行持續性的檢查

另外一個在導入 NAC 時所必須注意的問題是，早期的 NAC 解決方案，通常對於使用者的檢驗只有在第一次連線使用網路時，不管是使用 VPN 進入公司內部網路、採用 802.1x 的使用者登入機制或者透過 DHCP 獲得 IP 時才進行檢驗，因此投機的使用者可以在第一次連線時更改設定以符合公司安全性政策，一旦檢驗成功後再更改設定或者移除、安裝特定軟體，藉以規避檢驗，所以新的作法是採取定時或者不定時的檢驗，以查驗這些使用者可能的投機手段。

## 結論

NAC 的解決方案經過這幾年的發展已趨成熟，並達到實用的階段，新的 NAC 的技術具有下列幾點重要特性，：

- 1). 可以採閘道型、搭配 802.1x 或者使用 DHCP 模式
- 2). 使用者可選擇安裝用戶端軟體、Agentless 或者使用 ActiveX，並支援多種作業系統。
- 3). 檢驗的項目可達數百種，檢驗的時間不超過 15 秒並可自行定義檢測的內容。
- 4). 可於背景進行持續性的檢驗。

管理階層在導入 NAC 解決方案時可依這幾點特性作為參考，慎選廠家及解決方案，方可高枕無憂而非另一個夢靨的開始。