Windows DNS 更改為校內 Cache Only Server 設定

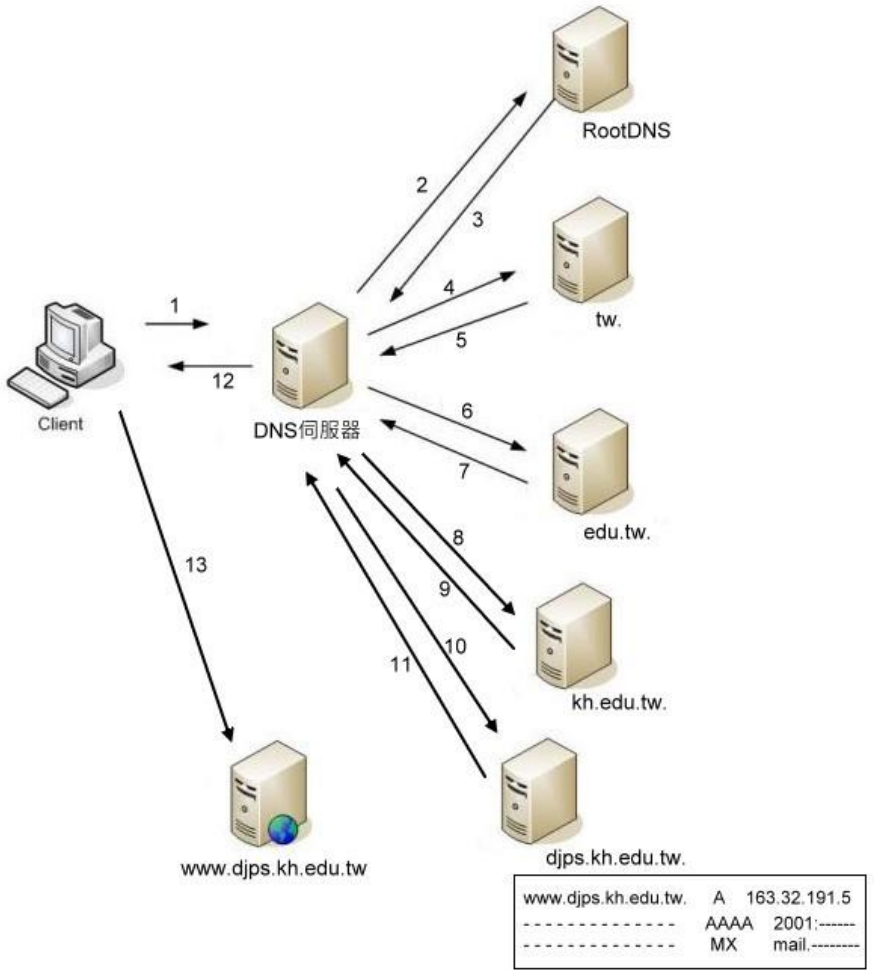
壹、說明
貳、更改學校已授權的 zone 由資教中心 DNS 代管
參、修改 Windows DNS 只服務校內 client，擔任 Cache Only DNS Server
肆、修改出口防火牆規則

壹、說明

一、DNS 查詢分為 2 種型態，

A：遞迴查詢（recursive query），如下圖中，編號 1 由 Client 對 DNS 伺服器提出的查詢，為 recursive query，DNS 伺服器會先由 Cache 中尋找要查詢的紀錄，若 Cache 中找不到，則會向其它 DNS Server 查詢，再將查到的結果回傳給 Client。

B：反覆查詢（iterative query），如下圖中，編號 2 到 11 由 DNS 伺服器之間的查詢，屬於 iterative query。



二、目前常發生的攻擊事件，為攻擊者利用已被控制的殭屍電腦群向開放遞迴查詢（recursive query）的 DNS 伺服器發出大量的遞迴查詢（recursive query），DNS 伺服器必須轉向 RootDNS 及其它 DNS Server 查詢後，向已被控制的偽造來源主機回傳 domain 查詢資料。
透過不斷的大量遞迴查詢，向目標 DNS 主機發送大量 UDP 封包，藉此阻斷正常網路，若接受遞迴查詢的 DNS Server 有設定 Forward 到資教中心的 DNS Server，會演變成攻擊資教中心 DNS 的狀況。

三、避免此種攻擊手法的方法為將 DNS 伺服器的遞迴查詢（recursive query），限制在僅提供校內電腦 ip 可以查詢、不開放其它外部 ip 查詢。

四、Windows DNS 在遞迴查詢上，無法設定可查詢 ip 範圍，僅能關閉或開啟遞迴查詢功能。為提供校內電腦 DNS 查詢服務，無法關閉遞迴查詢功能，所以只要有開放遞迴查詢功能的 Windows DNS 主機，必須只服務校內主機，不開放外部的查詢，亦即僅做為提供校內主機查詢的 Cache Only DNS Server。

五、學校已經由資教中心授權的 zone，必須接受外部的查詢，才能讓學校外部主機使用 FQDN 連線到校內伺服器。授權的 zone，可以直接申請資教中心的 DNS 代管服務，因資教中心的 DNS 伺服器，僅接受本市的 ip 連線進行遞迴查詢(recursive query)，安全機制比較完整。原本已經在運作的 Windows DNS，就在校內提供校內主機的查詢，擔任 Cache Only DNS Server 的角色。

六、由於運作的 Windows DNS，僅在校內提供校內主機的查詢，所以在出口端的防火牆，亦須關閉原本開放的由外對內部 Windows DNS 的 UDP 及 TCP 53 port。

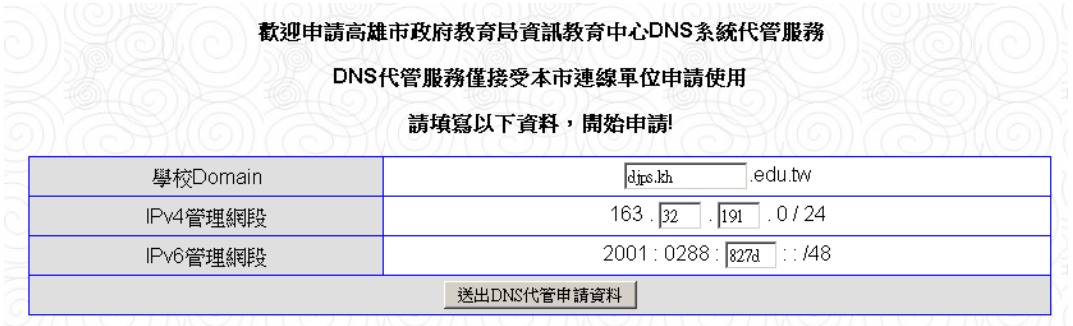
貳、更改學校已授權的 zone 由資教中心 DNS 代管

此步驟，只要進入資訊服務入口申請 DNS 代管服務，送出申請資訊後，由網路組設定，將學校的 zone 改回由資教中心的 DNS 代管，修改完成後，會 mail 通知執秘老師。開通 DNS 代管服務之後，請老師將原本 Windows DNS 上的紀錄加入 DNS 代管介面中即可。

一、由瀏覽器輸入 https://portal.kh.edu.tw -> 業務網站 -> DNS 代管

二、點選”申請 DNS 代管服務”，開始申請

三、填寫學校 Domain、v4 網段、v6 網段，送出申請資料，等候網路組設定完成後，會以 mail 通知（若不清楚 ipv6 資訊，請任意填入 0-f，網路組會校正）



四、收到開通郵件，確認開通 DNS 代管服務後，請登入 DNS 代管，將原本在 Windows DNS 上學校的正解紀錄、v4 反解紀錄、v6 反解紀錄加入資教中心的 DNS 代管介面中，便完成 DNS 代管動作

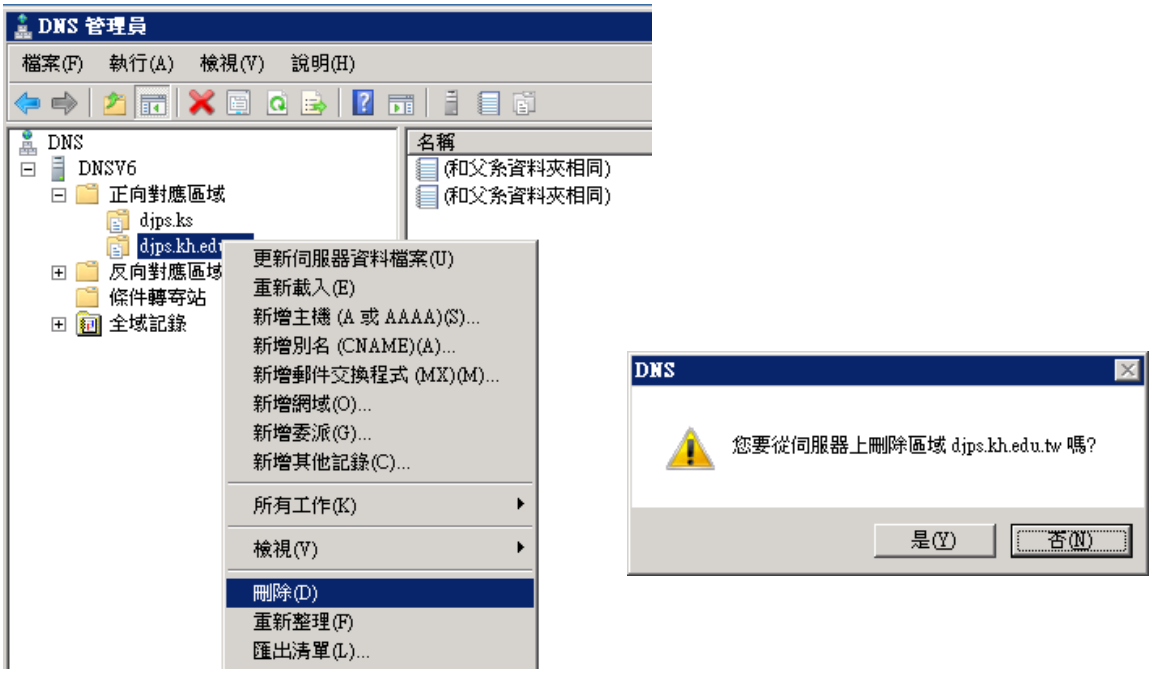
參、修改 Windows DNS 只服務校內 client，擔任 Cache Only DNS Server

此步驟有 2 種狀況，一為沒有使用 Windows AD 的 DNS，另一種狀況為校內有使用 Windows AD 的 DNS

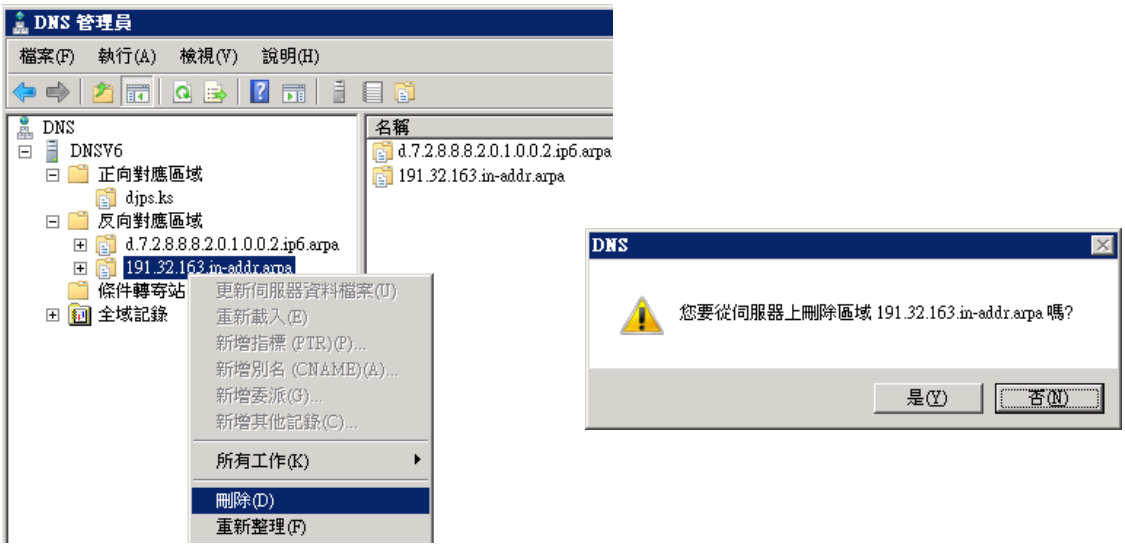
一、沒有使用 Windows AD 的 DNS

由於原本在 Windows DNS 上管理的學校正解、v4 反解、ipv6 反解已經轉移到資教中心的 DNS 上，所以只要將 Windows DNS 上已經轉移到資教中心代管的正解區域、v4 反解、ipv6 反解刪除即可

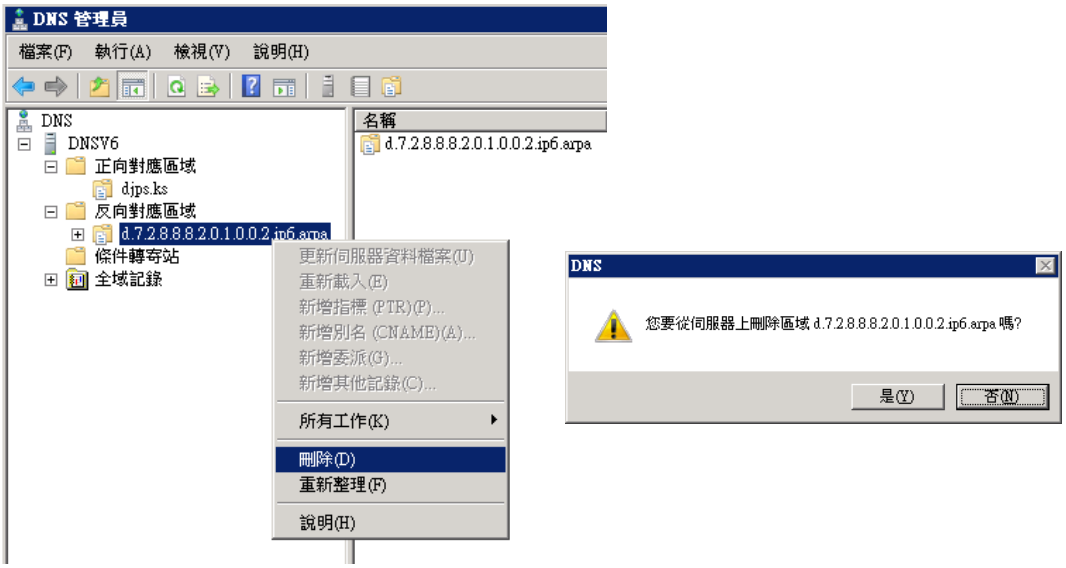
1、刪除 Windows DNS 上的正解區域，請展開正向對應區域 -> 選擇已經設定到資教中心 DNS 代管的 zone -> 右鍵 -> 刪除 -> 是



2、刪除 Windows DNS 上的 v4 反解，請展開反向對應區域 -> 選擇已經設定到資教中心 DNS 代管的 v4 反解區域 -> 右鍵 -> 刪除 -> 是



3、刪除 Windows DNS 上的 v6 反解，請展開反向對應區域 -> 選擇已經設定到資教中心 DNS 代管的 v6 反解區域 -> 右鍵 -> 刪除 -> 是



二、使用 Windows AD 的 DNS

如果校內有部署 Windows AD 網域環境，因 Windows AD 必須經由 DNS 查詢服務才能正常運作，所以不可刪除原本 AD 上的 DNS 區域。

但是原本 Windows DNS 上管理的**學校正解**、**v4 反解**、**ipv6 反解**都已經轉移到資教中心的 DNS 代管主機上，所以必須保持資教中心 DNS 代管上的**學校正解**、**v4 反解**、**ipv6 反解中**的紀錄，和 Windows DNS 上管理的**學校正解**、**v4 反解**、**ipv6 反解**中的紀錄都一模一樣。

亦即若是日後修改 Windows DNS 上的紀錄，必須同時上 DNS 代管介面上修

改相同的紀錄，讓 2 邊的紀錄都保持一致，校內、校外主機在查詢學校記錄時才會保持一致，不會有問題。

肆、修改出口防火牆規則

經由前面步驟，已經讓原本的 Windows DNS 僅提供校內主機的 DNS 紀錄查詢，已經授權的學校 domain，就交給資教中心的 DNS 代管主機接受外部的查詢。

由於 Windows DNS 僅服務校內主機，所以原本在學校出口端的防火牆（juniper 或 vSYS）上，開放由外部對內部 Windows DNS 的 TCP 及 UDP 53 port 的規則必須停用。

請經由電話聯繫（7136536#16）或線上報修系統留言，讓負責防火牆的工程師邱先生，協助停用此規則。

(本篇文章, 由侯人俊老師撰寫提供)