DNS劫持事件層出不窮　解析明文傳輸成攻擊標的

路由器層級DoH兼顧防護 加密杜絕瀏覽紀錄曝光

在網路威脅層出不窮的時代，網路安全一直是個重要的議題。隨著DNS劫持事件頻傳，DNS over HTTPS（DoH）也成為關注焦點，本文將有詳細說明這項正在逐漸瓦解網路供應商及政府機關之既有網路運作模式的新技術，將帶來哪些好處與影響，以及如何將其應用在設備的隱私保護上。

近年來，全球DNS劫持事件頻傳，DNS over HTTPS（DoH）也在2019年成了新聞頭條的熱門字眼。繼Google在六月宣布正式支援DoH後，緊接著七月，Mozilla因為在Firefox上支援DoH，被英國網際網路服務供應商聯盟（ISPA）點名為2019網路惡霸（後來該提名因為全球撻伐而被撤除），這象徵著一項新技術正逐漸瓦解網路供應商及政府機關的既有網路運作模式。接下來，就來看看DoH有什麼好處、對於我們所依賴甚至為之付費的服務又帶來哪些影響，透過這項最簡易且不須改變既有使用習慣的方法，在所有的裝置上使用這個強調「隱私至上」的技術。

DNS over HTTPS：照亮網路隱私的未來

現今多數熱門網站都使用HTTPS來加密連線，保護如密碼、信用卡資訊與網路銀行登入等敏感資料。但是，DNS解析還是以明文進行傳輸。舉例來說，假設在瀏覽器上輸入blog.synology.com，此搜尋會聯

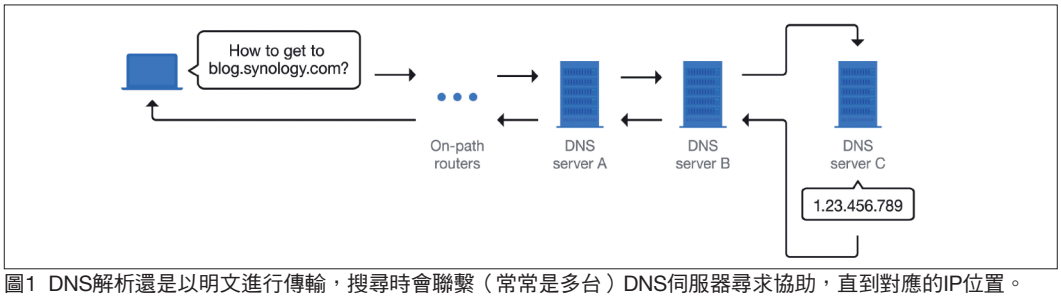

圖1 DNS解析還是以明文進行傳輸，搜尋時會聯繫（常常是多台）DNS伺服器尋求協助，直到對應的IP位置。

作者：
陳家敏
群暉科技產品行銷經理，2013 年加入群暉科技，在群暉科技負責儲存技術、網路解決方案之產品行銷管理。

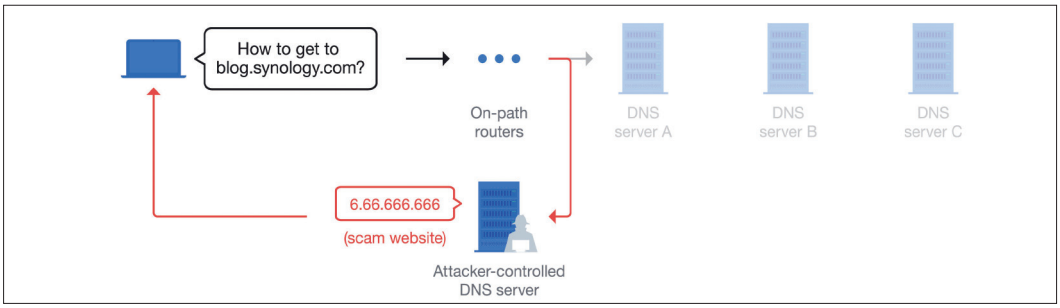

圖2 一旦能查看到DNS要求，也就代表有心人士能竄改回應，重新導向至詐騙網站。

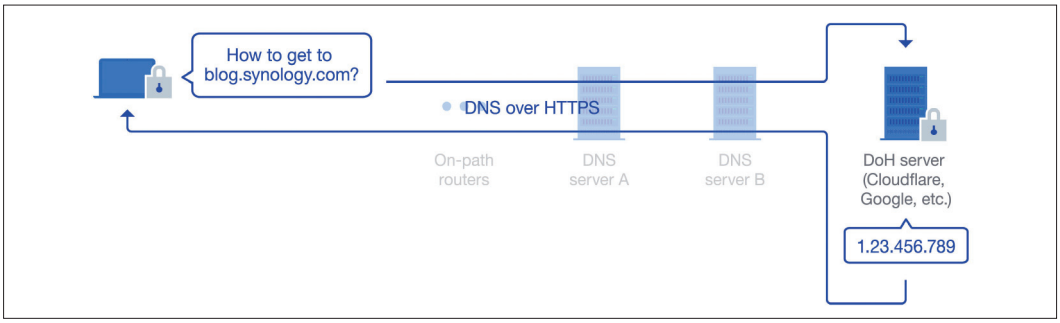

圖3 DNS over HTTPS主要是透過加密DNS來避免他人窺探或將流量導入至惡意網站。

繫（常常是多台）DNS伺服器尋求協助，直到找到與網域blog.synology.com（例如1.23.456.789）對應的IP位置，如圖1所示。

因為DNS是以明文傳輸，相關的DNS伺服器（例如網路供應商的伺服器）以及任何此路徑中的路由器都可以知道拜訪了哪些網站。一段時間後，這些瀏覽紀錄就會成為網路活動的完整寫照，並可能被使用於廣告推銷。一旦能查看到DNS要求，也就代表有心人士能竄改回應，重新導向至詐騙網站，這就是所謂的「DNS劫持」，如圖2所示。今年四月很多人就因此被騙交出自己的PayPal、Netflix、Gmail與Uber的登入資訊。

而DoH是透過HTTPS加密所有的DNS解析，因此只有DNS用戶端（瀏覽器）與所選用的DoH伺服器才會知道拜訪過哪些網站，其他人不得其門而入，這能有效避免他人窺探或將流量導入至惡意網站（圖3）。

隱私vs.內容過濾

目前為止，包含Google、Cloudflare以及其他數間公共DNS服務商都已開放DoH服務。Mozilla也和Cloudflare合作，讓Firefox使用者能透過DoH保護日常的網頁瀏覽。既是如此，為什麼Mozilla會被英國的網路供應商稱為「網路惡霸」呢？

首先，某些國家的網路供應商因受到法律規範，必須保留用戶的瀏覽紀錄達一段時間（如12個月）以助於犯罪調查，若DoH變成主流，這恐成為一大阻礙。這也讓網路供應商難以提供須付費的家長監護與安全防護服務，因為他們無從查看並攔截DNS解析，而讓成人、惡意網站得以隱藏形跡（圖4）。

其實，受影響的不單單只有網路供應商。透過DNS進行內容過濾非常普遍，幾

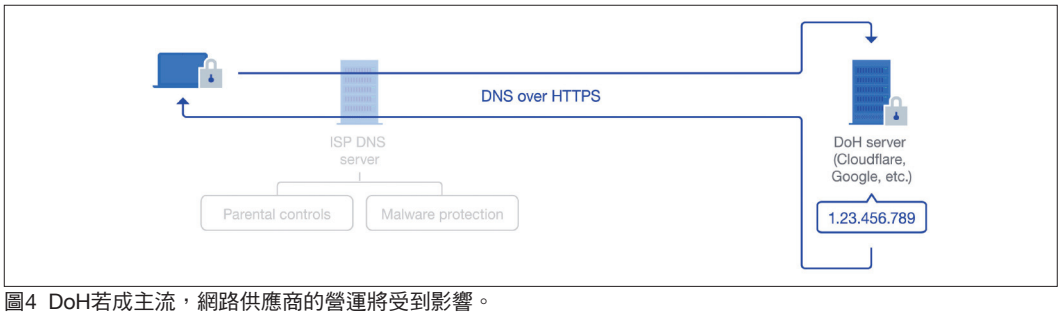

圖4 DoH若成主流，網路供應商的營運將受到影響。

乎每個安裝在網路中的家長監護裝置都使用它，而許多安全產品也透過它作為一種低誤判率的辨識威脅方式。如果DNS解析在通過這些產品前就被加密，那這些產品也就無用武之地了。

而這也是為什麼在一開始就提到DoH正瓦解既有的網路運作模式。現階段，要享受這項技術所帶來的好處可能還需等上一段時間，大部分的應用程式與作業系統（(Windows、macOS等）都不具原生DoH支援。若要設定，通常需要透過命令列工具，而且每一個希望被保護的裝置都要個別設定一遍。

導入路由器層級DoH

一般情況下，若設定裝置時遇到繁瑣、重複的程序，直覺上就會把它們移到路由器層級來解決，而這也是Synology路由器上的Safe Access與Threat Prevention誕生的原因，關鍵就在能一次完成網頁過濾、安全搜尋以及網路保護等需求。如今許多無法進行複雜設定的裝置（如IoT裝置）數量不斷攀升，這些功能便更顯重要，相同道理，在路由器作業系統導入了DoH，意味著每當裝置上的DNS解析通過路由器時，都會透過HTTPS進行加密。如今，使用者只需在SRM上選用偏好的DoH伺服器（Google、Cloudflare，或輸入任何DoH伺服器網址），透過簡單的幾個點擊，就可以保護使用者的整個網路遠離他人窺探，如圖5所示。

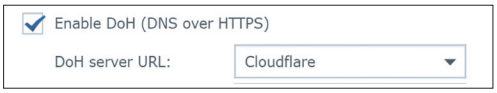

圖5 一個勾選方塊，即在所有連接裝置生效。

因為DNS解析只有在通過路由器時會被加密，Safe Access中的DNS威脅情報與安全監護功能得以持續作用。舉例來說，如果網路使用者無意間造訪管理者提前設定禁止的網站，路由器將會攔截此DNS解析並顯示自訂的訊息，而其他正常的搜尋則會被加密，他人無法將其瀏覽歷程紀錄作為非法用途使用，如圖6所示。

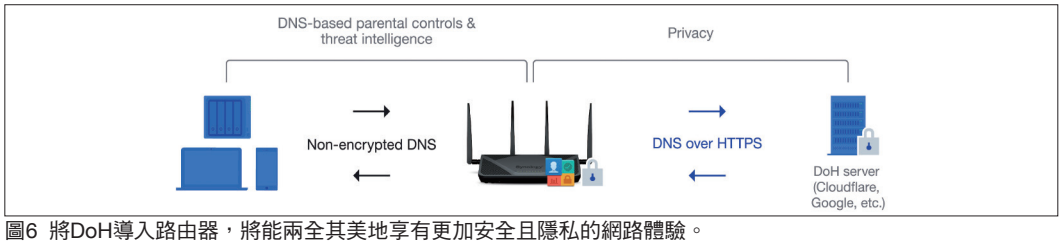

圖6 將DoH導入路由器，將能兩全其美地享有更加安全且隱私的網路體驗。