讓眾至郵件伺服器的SPF驗證和DKIM驗證幫我們過濾偽造信件!

SPF驗證及DKIM驗證會過濾掉哪些信件呢?

SPF驗證能幫我們過濾掉非法主機偽造合法網域寄出的信件，而DKIM驗證則能過濾掉在寄件過程中寄件者、主旨、內文、附件等部份被偽冒或竄改的信件。

試想一情境，使用者今天收到一封email，寄件者顯示是主管的email，信件標題為專案協作，信件內容可能是檔案及網址，使用者會不會點開呢?

你會想到email在傳送到你的信箱前，其實已經在中途被駭客攔截，將主管的信件內容竄改過，並附上惡意程式網站連結嗎?

甚至有可能email一開始就是由不合法的伺服器發送，只是將寄件者改為使用者信賴的email及網域，加上合理的信件標題，內文再附上釣魚網站網址。收到這樣的偽造信件，上當的機率幾乎是百分之百。像這樣偽造寄件者或被竄改內容的偽造信件，我們能不能在還沒進入使用者信箱前，就過濾掉不讓使用者有機會開啟呢?

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

為什麼需要SPF驗證及DKIM驗證?

資安防護來說，電子郵件是最容易被駭客利用來入侵企業內部網路的管道。當email抵達使用者端時，使用者往往只會看到信件寄件人及信件主旨，就決定是否開啟此封信件，甚至大部分的使用者在收到email後，都會直接開啟信件。有些信件裡面附加的惡意程式點選後就馬上攻擊開啟郵件的設備，或者在背景盜取電腦資料，不只公司內的電腦有可能被當成跳板，嚴重的話，公司內的商業機密被盜取，甚至癱瘓公司重要聯網設備都有可能。

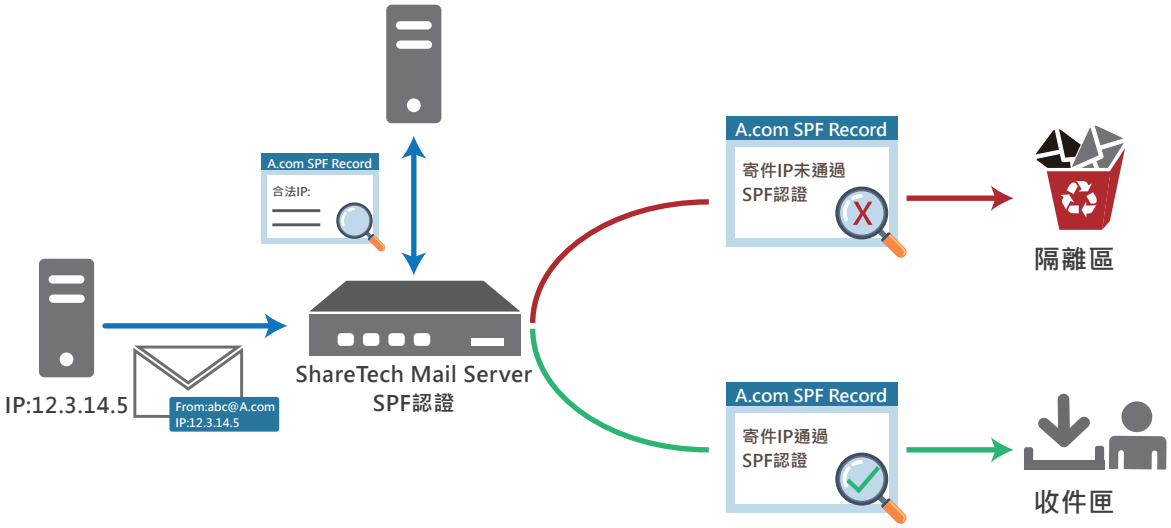
以目前最鼎鼎有名的wannacry勒索病毒為例，當使用者點擊了不明的網站或者檔案，可能就成為受災戶。所以我們更要在電子郵件抵達收件者信箱前，在郵件伺服器做好過濾及把關，避免員工一失手成公司的千古恨，您沒考慮到的，眾至郵件伺服器都幫您想好了!

SPF 驗證機制 Sender Policy Framework

網域DNS的SPF紀錄中會記錄允許用這個網域名寄信的主機，收件端郵件伺服器收到email後，會依據寄件者網域DNS查詢SPF紀錄，確認收到的信件是由寄件者網域許可的主機發送的，如果SPF紀錄上有寄件主機，則信件就會被視為合法信件，如果SPF紀錄上沒有寄件主機，則信件就會被攔下。

SPF運作流程範例:

Step1. MailServer收到來自" IP:12.3.14.5, 寄件者:abc@A.com" 的信件。
Step2. MailServer會依據寄件者網域,至A.com 的DNS比對SPF記錄。
Step3. 如果寄件主機IP:12.3.14.5在A.com的SPF記錄上，則Mailserver才會將信件收至收件匣。



除了去驗證寄件者是否合法外，我們寄出的信件也可以啟用SPF紀錄，將寄件主機增加到網域DNS的SPF記錄上，如果遠端收件者有開啟SPF機制，就可提供SPF記錄驗證，減少信件被視為垃圾郵件的機會。

DKIM驗證機制 Domain Keys Identified Mail

DKIM（網域認證金鑰）運用加密及簽章方式來認證信件的來源。原理是送件端在寄出信件時，會先用自身的私密金鑰對信件做DKIM簽章，收件端MailServer收到信件後，根據信件所標示網域，向DNS伺服器取得公開金鑰，再用公開金鑰驗證DKIM簽章，以確認信件來源的真實性，如果通過驗證，表示信件未受到竄改，則Mail Server才會將信件傳遞到使用者的收件匣。

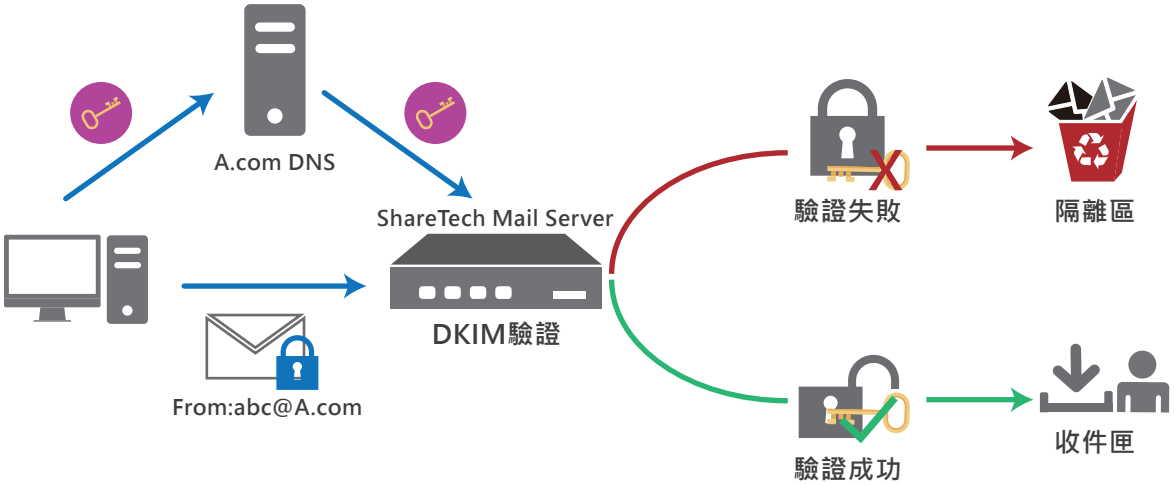
DKIM（網域認證金鑰）運作流程說明：

Step1. 送信端發送一封經過私密金鑰簽章的信件，並在信件標題中宣告網域A.com，同時將對應的公開金鑰發布至A.com的DNS。

Step2. MailServer根據信件標題中宣告網域，向A.com DNS伺服器取得公開金鑰。

Step3. MailServer利用公開金鑰對信件中的簽章進行驗證。

Step4.如通過驗證，表示郵件運送途中未經竄改，MailServer才會將信件傳至使用者收件匣。



註:DKIM簽章就是在所有對外的郵件，利用私密金鑰對郵件標頭及內容做加密動作，並產生特定格式的簽名檔附加於郵件標頭。收件主機將依據查詢到的公開金鑰，驗證這段簽名檔的正確性。