Sender Policy Framework

- Sender Policy Framework (SPF) 是檢驗寄件者(MAIL FROM)是否經由授權的 IP 位址(Sender IP address)寄信的一種架構。以下用簡單例子說明其運作方式如下：
  - 寄信者 user@cc.nthu.edu.tw 所屬網域的 DNS 管理者，先將 DNS 註冊該郵件網域所授權寄信的 IP 位址範圍。

```
# dig +short cc.nthu.edu.tw txt
"v=spf1 ip4:140.114.62.0/23 ?all"
```

  - 當寄信者 user@cc.nthu.edu.tw 將信件由本組 SMTP 伺服器之一的 IP 位址 140.114.63.4 (屬 140.114.62.0/23 範圍內) 寄給校外某郵件伺服器，若該郵件伺服器採用 SPF 的檢查，透過 DNS 查詢即可確認來源 IP 位址屬於授權範圍，則通過其檢查而順利寄達。
- http://www.openspf.org/
- 檢測寄件者(MAIL FROM) 由某 IP 位址(Sender IP address)是否為符合 SPF 授權寄信?
  - http://www.openspf.org/Why
- SPF 語法(DNS TXT紀錄)
  - http://www.openspf.org/SPF_Record_Syntax

實例說明

設定 SPF 以順利寄信至 Google 信箱

- 本校系所單位，**如欲使用本組寄信服務(包含SMTP或SMTPAUTH)寄信至 Google 信箱(例如@gmail.com, @gapp.nthu.edu.tw)建議其網域管理者將 SPF 設定加入 include:spf.net.nthu.edu.tw**(spf.net.nthu.edu.tw 內含本組所有寄信伺服器，如下，以寄信者網域 @mx.nthu.edu.tw 為例)，則較能順利寄達。**注意：若該系所單位還有其他寄信伺服器，記得一併加入設定中。**

```
# dig +short mx.nthu.edu.tw txt
"v=spf1 include:spf.net.nthu.edu.tw mx ?all"
```

  - BIND 格式

```
mx.nthu.edu.tw.         20M     IN      TXT     "v=spf1
include:spf.net.nthu.edu.tw mx ?all"
```

  - 其中 include:spf.net.nthu.edu.tw 表參考其資料，如下：

```
# dig +short spf.net.nthu.edu.tw txt
"v=spf1 ip4:140.114.62.0/23 ip6:2001:288:E001:63::/64 ?all"
```

- 若沒有 SPF 設定，則可能收到以下暫時錯誤訊息的通知信。

```
<xxxxxxx@gmail.com>: host gmail-smtp-
in.l.google.com[2404:6800:4008:c06::1b]
    said: 421-4.7.0 This message does not have authentication
information or
    fails to pass 421-4.7.0 authentication checks. To best protect our
```

```
users
    from spam, the 421-4.7.0 message has been blocked. Please visit
421-4.7.0
    https://support.google.com/mail/answer/81126#authentication for
more 421
    4.7.0 information. xxxx.xxx - gsmtp (in reply to end of DATA
command)
```

- 參考資料Authorize senders with SPF https://support.google.com/a/answer/33786