該如何預防郵件伺服器短時間被大量垃圾郵件攻擊?

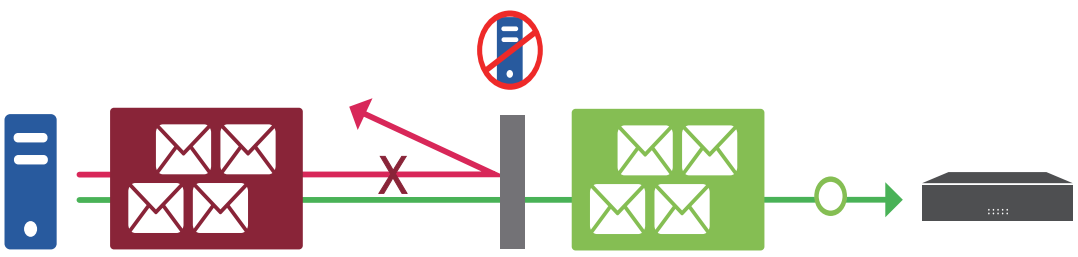
當郵件主機收到大量垃圾郵件，會造成郵件處理效能低落，儲存空間也會因為被大量垃圾郵件佔據造成無可用空間，無法再接收到真正重要的電子郵件。當本機內部帳號被猜中密碼，也有可能在短時間內寄送大量垃圾郵件，不論是收到大量外部垃圾郵件，或內部帳號寄出大量郵件，都是郵件主機該阻止的異常行為。眾至郵件伺服器的郵件防火牆SMTP流量異常偵測功能，可以偵測所有SMTP流量異常的情況，當內送信件或是外寄信件觸發限制值，即自動封鎖寄件來源，及時阻止郵件主機被短時間密集信件攻擊的問題。

郵件防火牆 — SMTP流量異常偵測

郵件管理員可依照來源IP、認證帳號或寄件者自訂偵測規則，並可自訂時間間隔及信件數量，只要短時間內信件數量超過任一偵測規則限制值，即進行封鎖，使郵件主機能及時阻擋郵件異常狀況。

短時間內，同一來源IP、認證帳號或寄件者寄出之信件如超過信件數量限制值，即進行封鎖:

1. 外部郵件伺服器發送大量垃圾郵件，同一IP來源寄送過多郵件超過限制值，針對IP進行封鎖。

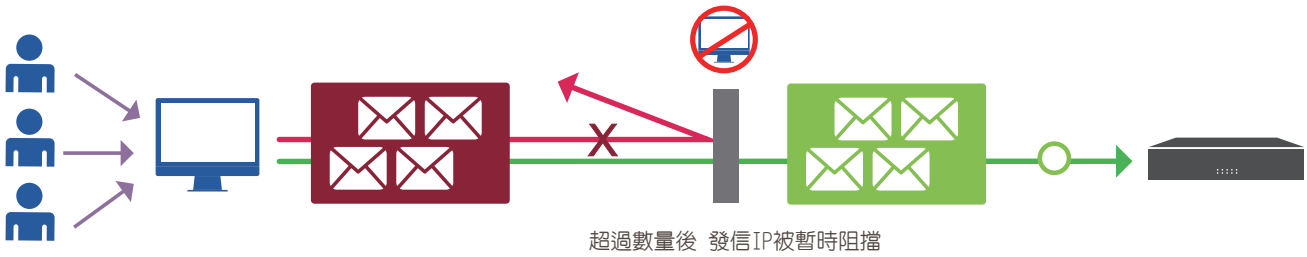


超過數量後 發信伺服器被暫時阻擋

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

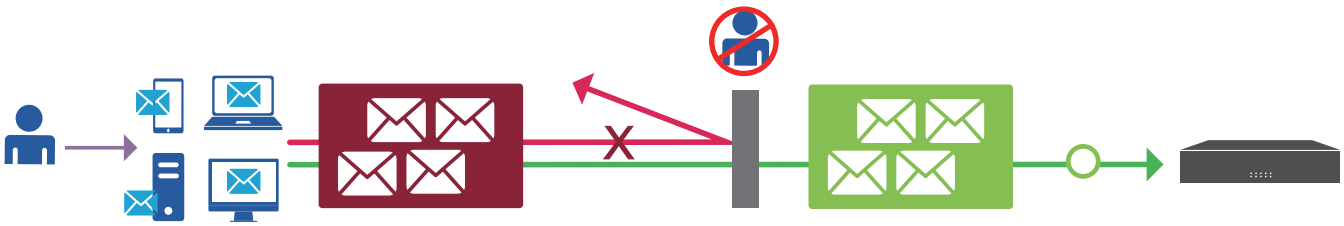
該如何預防郵件伺服器短時間被大量垃圾郵件攻擊?

2. 多個不同寄件者或帳號，由同一台內部電腦寄送過多郵件，雖然寄件者各別寄出信件數量未達限制值，但此台內部電腦IP累計寄出信件超過限制值，則針對此內部電腦IP進行封鎖。



超過數量後 發信IP被暫時阻擋

3. 同一SMTP認證帳號或寄件者，使用不同IP的裝置寄送過多郵件，則針對其SMTP認證帳號或寄件者進行封鎖。



超過數量後 發信帳號或寄件者被暫時阻擋

SMTP流量異常偵測設定

1. 登入Mail Server 管理介面後，至 [郵件稽核及防護] > [郵件防火牆]。
2. 將視窗拉至SMTP流量異常偵測，即可對各項異常偵測限制值進行調整。
3. 當寄件端觸發來源IP、認證帳號或寄件者偵測規則限制值，三項其一觸發即會封鎖此封信件。

偵測順序: 來源IP → 認證帳號 → 寄件者，當項目已被封鎖時，就算後者項目有設為例外，結果仍然是封鎖。

- 依據來源IP: 當同一來源IP位址(外部郵件伺服器或企業內部電腦固定IP)，發出的郵件數量觸發[偵測IP規則]，則封鎖此來源IP位址寄出的信件。

- 偵測IP規則 : 秒數限制及郵件數量限制皆可自訂，可自訂時間間隔內的限制郵件數量，當數量超過限制值則會封鎖此來源IP寄出的信件。

- 依據認證帳號 : 當同一內部認證帳號，發出的郵件數量觸發[偵測認證帳號規則]，則會封鎖此內部SMTP帳號寄出的信件。

- 依據寄件者 : 當同一寄件者，發出的郵件數量觸發[偵測寄件者規則]，則會封鎖此寄件者寄出的信件。