新軟週報
http://www.nusoft.com.tw
Internet Security Fighter
2009/11/30- 2009/12/13 第106期

郵件伺服器 / ML 系列報導

技術淺談與應用 - 自動化白名單

數位 e 化的時代，垃圾郵件問題，長久以來一直是所有人的困擾，在目前無法完全治本的情況下，只能靠治標的方向來解決，利用科技來圍堵垃圾信將是企業自保首要之道。因此反垃圾郵件技術不斷翻新，在眾多防護機制中，比對式垃圾郵件過濾方式又是最為基本不可缺的一項。比對過濾技術大概可分兩種類型，傳統也是大多企業使用的是「名單比對」（如黑、白名單）。其中黑名單是攔阻垃圾郵件最常用之過濾方式，基本上利用人工鍵入方式來判斷是否為垃圾郵件來源，郵件伺服器再依據黑、白名單上所鍵入之清單來判斷處理。

“黑名單”是指一個事先的郵件篩檢方式。雖然被最廣泛地用以對抗垃圾郵件的解決方案，但有時它不但不能夠有效阻止垃圾郵件，而且還可能會導致了一些合法並重要的電子郵件永遠都不能到達目的地。相對和黑名單基於排除的做法不同，“白名單”是致力於確認合法之電子郵件來源，這樣就不會有黑名單排除失誤之情況，但卻有可能因為垃圾郵件利用偽造寄件來源的方式，而出現漏洞。

為彌補垃圾郵件黑、白名單防護機制舊有的不足之處，同時還可再配合其他郵件過濾機制，新軟系統推出了新式防護機制『自動化白名單』，來有效減輕管理人員對於垃圾郵件阻擋上的負擔。何謂『自動化白名單』？其運作方式又為何？以下將一一說明。

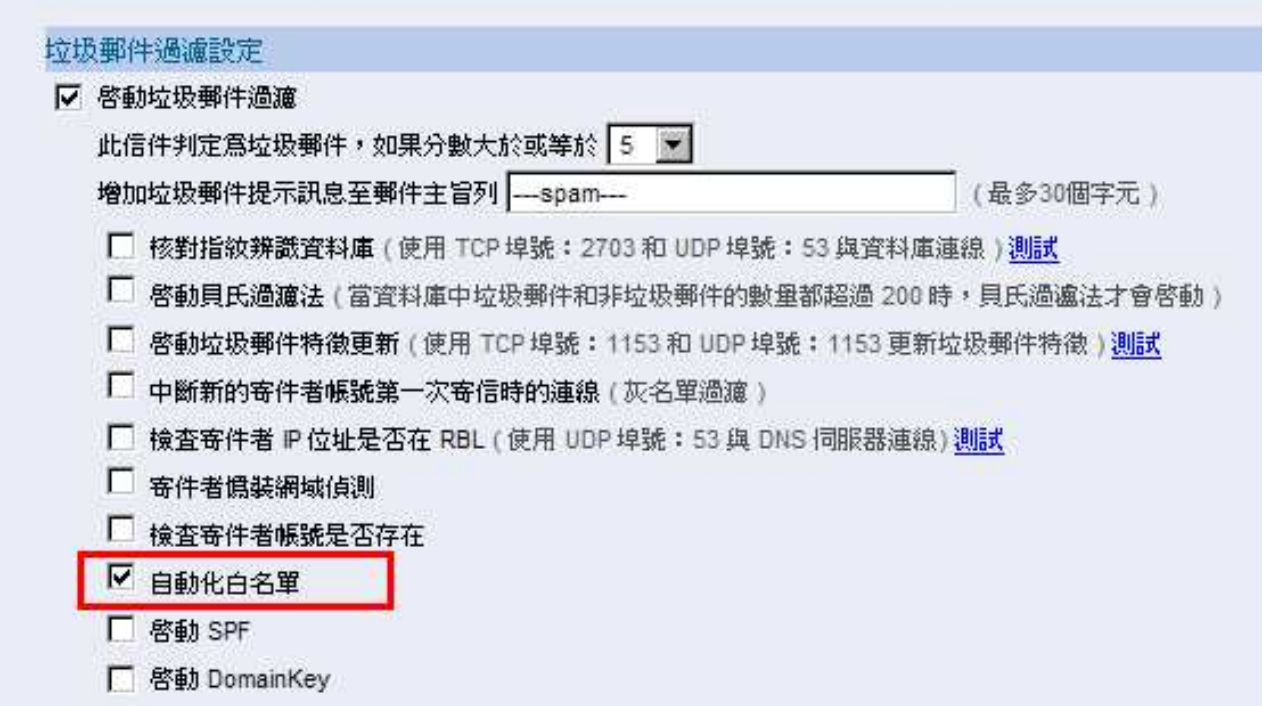
一、何謂自動化白名單：

簡單的說，自動化白名單是依照該寄件來源以往的記錄，進而來計算新信件是否為垃圾郵件之機率。當寄件者寄出一封信件到郵件伺服器 -ML 時，會先經由其他過濾機制過濾評分，最後再由『自動化白名單』機制計算這封信的評等，分數若越高，則代表該封信件之內容越符合垃圾郵件的定義。有別於平常一般所使用的黑、白名單之處在於管理人員可不必費心思去自行設定黑、白名單中的來源清單，即可藉由自動化白名單機制來達到有效的黑、白名單防護機制功能，同時還可大幅降低一般黑、白名單所易產生之信件誤判情形發生。

但管理人員必須要注意到，若於 ML 裡黑、白名單上有鍵入之名單，系統則會先行依照黑、白名單來做阻擋及放行，該些名單並不會再由『自動化白名單』機制來進行處理判斷與計算。

二、如何啟用自動化白名單：

管理人員可在 ML 系統中『郵件安全 > 郵件過濾 > 設定』下，於『垃圾郵件過濾設定』中勾選『自動化白名單 』後，即可啟用。



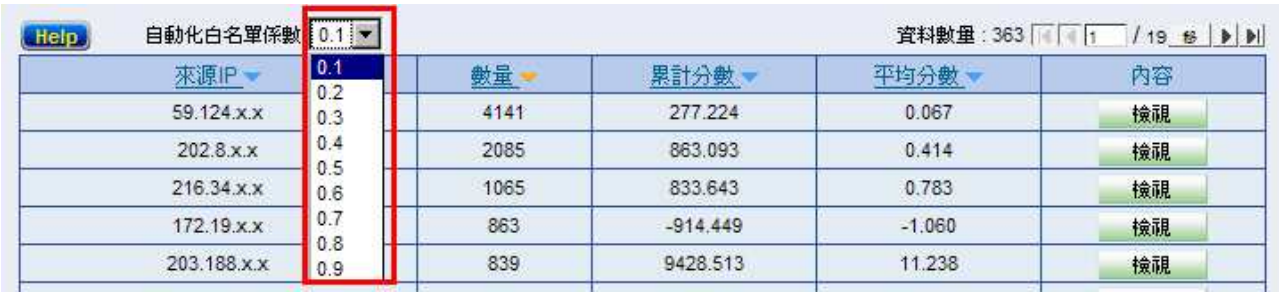
開啟自動化白名單機制

三、自動化白名單中的來源判斷方式：

『自動化白名單』機制會記錄所有寄件者的 e-mail 和 class B 的 IP 位址，每當有新信件時，則系統會去比對這兩個欄位，若兩個欄位資訊皆相同系統才會將該信件視為同一個寄件來源。之後再依據來源做分數的計算與累計，這樣定義方法，可以避免垃圾郵件隨機假冒他人之 e-mail 帳號或者 IP 發出垃圾郵件，而造成該帳號或網域被誤列為黑名單。

四、自動化白名單上的『係數』用意：

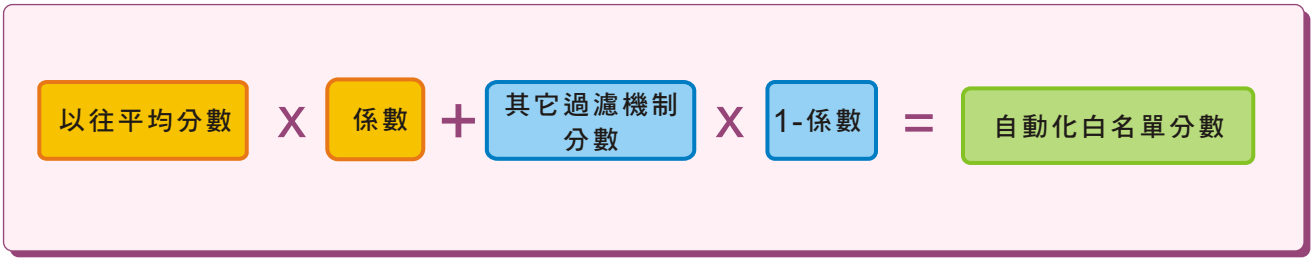
每有新信件送達時，自動化白名單機制就會將該封信件來源於機制裡以往所算出之平均分數(累計分數/累計信件數)和新信件的分數(其他過濾機制所算出)，依自動化白名單係數做權重分析。而當管理人員所設定之係數數值越高，則表示該來源之前於此機制中所計算出之平均分數佔有的權重越高，也就是說越重視該郵件來源先前所算出的分數結果。所以自動化白名單上的係數 0.1~0.9，也可以說成每次在做分數上的計算時，先前所算出之結果於該次分數運算中所佔的權重比例為 10%~90%。



自動化白名單的係數選單

五、自動化白名單的分數計算：

在自動化白名單機制中，新進信件的分數計算方式為『(先前平均分數x係數) + 〔新進信件分數 x (1- 係數)〕』，若是該來源無先前平均分數則會將其他過濾機制分數直接列入。如此計算機制有什麼好處呢？在這樣的機制下，當紀錄裡一個不曾寄送垃圾郵件之來源，新寄出的信件在垃圾郵件分析後分數若出現偏高時，機制會因為之前平均分數的良好紀錄，自動調降信件在垃圾郵件定義下之分數，以防止不當的誤判發生。例如當管理人員將自動化白名單上之係數設定為 0.4 時，某平均分數為 -5 分的良好來源，新寄出了一封分數為 10 分的信件時，先前良好的平均紀錄會乘上 0.4，而新信件的分數則會佔去另外的 0.6，[(-5) x 0.4] + (10 x 0.6)=4，分數則會被降低為 4 分。



信件計算示意圖

相反地，當一個常常寄出垃圾郵件的來源，就算本次寄出的信件在垃圾郵件的評等中分數偏低時，也會因為先前的不良紀錄而使得最後計算出之分數變高，藉此來提升該信成為垃圾郵件的可能，以防止不正常之信件因此而流入內部。例如當管理人員將自動化白名單上之係數同樣設定為 0.4 時，平均分數為 20 分的不良來源寄出一封分數 2分的新信件時，在 (20 x 0.4) + (2 x 0.6) 計算後，分數則會被提升為 9.2 分。

此外，自動化白名單中的分數表達方式為小數點以下第 4 位，四捨五入。

文 陳殿鴻 kim@nusoft.com.tw

市場行銷報導 - 新增功能「自動化白名單」，給您更聰明的郵件過濾機制

在現代這個數位化的時代，網路改變了人們的生活方式，隨之而來的便是e化之方便生活方式；但是從相反面來看，許多現實生活中讓人煩惱不已之行為也隨著生e化而衍生出來；最為明顯的行為莫過於“企業最為倚重之電子郵件”的垃圾郵件問題。

電子郵件是企業與企業之間最為倚重之商業往來工具，然而有利必有弊，其強大方便的功能性也被不肖份子所看中，被人拿來利用成為廣告垃圾信件的最佳途徑，導致現今廣告信件肆虐，常常讓人在一堆廣告信件裡找不到真正那封自己想要的瀏覽的信件，間接造成企業營運資源多餘浪費、公司生產效率降低…。基於以上多項企業間困擾的問題所在，使得市面上出現許多擁有垃圾郵件過濾機制的郵件伺服器。

但是目前市面上許多的郵件伺服器所提供之垃圾過濾機制大多都不夠完善、不夠人性化，最常見的方式是採用黑、白名單、RBL黑名單、貝式過濾…等幾種垃圾郵件過濾機制，然而單單就只依靠此幾類判別機制容易造成信件漏擋，甚至是信件誤判…等問題；因此新軟系統郵件伺服器-ML系列則提供使用者以獨家七道垃圾郵件過濾機制來嚴格把關，但是網路世界、一日千里，垃圾郵件也隨之變化多端。所以為了因應如此變化巨大的垃圾郵件類型，新軟系統郵件伺服器-ML系列又推出了“自動化白名單”此項聰明人性化之設計，藉以盡濾所有的垃圾郵件。

※自動化白名單

將以往之信件（來源與寄件者帳號）作為參考依據，再依所設定的係數做權重分析，以阻擋偽造寄件者之垃圾郵件（寄件人為自己的垃圾郵件），並可避免經常往來之寄件者的來信被誤判為垃圾信。（詳細計算方式，請參閱本期技術篇）

新軟系統藉提供此功能讓使用者在白名單使用上更為輕鬆方便，也讓垃圾郵件在新軟系統郵件伺服器7+1的八道垃圾郵件過濾機制裡更加無所遁形，讓企業資安處理能力更為完善、企業營運更具實力。

	使用時機
黑名單	不請自來的電子報。 （固定寄件者帳號之垃圾信件）
白名單	信件往來的廠商、客戶。 (不建議將企業網域整個加入白名單，此種設定會造成無法阻擋偽裝成內部寄件者之垃圾信件)
自動化白名單	1.偽造成內部寄件者之垃圾信件 2.企業內部往來之正常信件被誤判時。

新軟郵件伺服器黑名單、白名單與自動化白名單使用時機

文 黃政銘 ming@nusoft.com.tw