

大型企業整合運用 應用範例

你
·
簡
單
用
網
路
·
複
雜
問
題
我
們
處
理
!

■ UTM 異常發送郵件偵測及阻擋

垃圾郵件的發送技術越來越進步，網路的使用者往往不知道自己已經受害被當成垃圾郵件的跳板而不知。

傳統的firewall或是UTM甚至 IDP並沒有辦法阻擋這樣的行爲，因為從網路的觀點，這是管理者允許的網路行爲，一旦 ISP 業者發現並封鎖 對外 IP時，才去找LOG紀錄，分析那一個設備才是跳版。

UR的異常發送郵件偵測及阻擋將這一方面的技術發揮到極致，一旦有人被當跳板，立刻阻擋。

偵測

一般正常人發信不會在短短的時間內發送大量的信件，利用這個特徵值，管理者可以設定防禦機制。

假設UTM 在100秒內收到同一個來源 IP或是帳號對外發送超過10封信，就可以認定他是被植入木馬(因為按照一般使用者信件寄送情況，在一分鐘內寄送超過3封以上之信件，都是算寄送量很大之使用者。所以我們可以假設判定當使用者在100秒裡面寄送超過10封以上之信件，我們就可先判斷此為不合理現象)，此時將對外發信的動作阻擋特定時間。

The screenshot shows a configuration interface for UTM. At the top, there are four tabs: '郵件過濾及紀錄', '有效帳號設定', '灰名單設定', and '流量封鎖防禦設定'. The '流量封鎖防禦設定' tab is selected. Below the tabs, the '流量封鎖防禦' section is expanded. It contains a '規則設定' (Rule Setting) section with the following values: '100' for '秒內 達到信件量為' (seconds to reach message volume) and '10' for the message count. Below this, '每次封鎖時間(秒)' (Blocking time per message in seconds) is set to '600'. At the bottom, there is a section for '依據寄件者封鎖' (Block by sender) with two radio buttons: '啟動' (On) and '關閉' (Off), where '關閉' is selected.

大型企業整合運用 應用範例

你
·
簡
單
用
網
路
·
複
雜
問
題
我
們
處
理
!

封鎖

2種封鎖機制

1.依據寄件者封鎖

計算的依據是寄件者，例如，用123@abc.com 對外狂發不特定收信者的信件，才會列入統計。

2.依據 IP位址封鎖

計算的依據是寄件者的ip位址，例如，192.168.1.100使用不特定的寄件者名稱對外狂發不特定收信者的信件，才會列入統計。

所有的攻防紀錄都會被系統記錄下來。