Email Technical Document

允許外部發送同網域郵件到公司內部

郵件技術白皮書
《沛盛資訊》

《沛盛資訊》有限公司
台北市內湖區瑞光路 188 巷 46 號 5 樓
(02)7720-1866
contactus@itpison.com
https://www.itpison.com

TABLE OF CONTENTS

1. 寄件者與寄件人

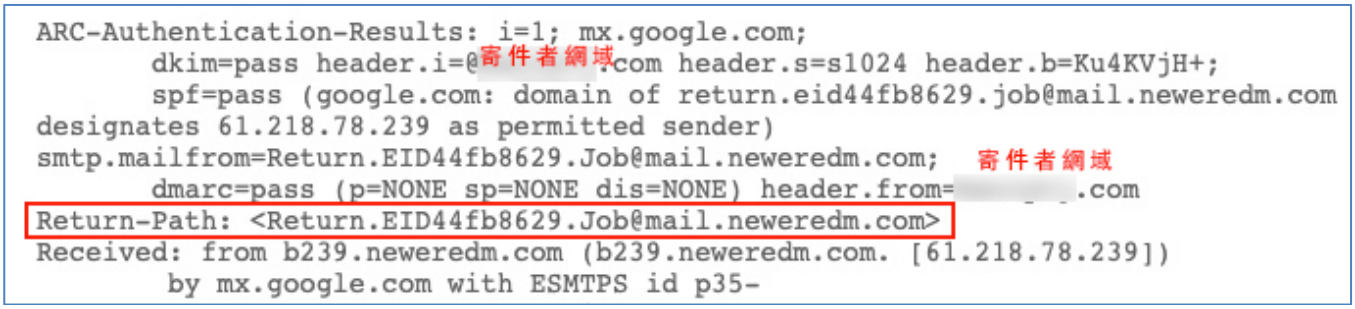
A. 寄件者與寄件人差別

一般而言由《沛盛資訊》雲端電子報所寄出郵件，寄件人MAIL FROM為 mail.neweredm.com。

寄件人FROM並非讀信程式可見之"寄件者"。參見下圖Gmail收信示範，"寄件者"為讀信程式可見發信人郵件地址。"寄件人" MAIL FROM 則為郵件寄送SMTP服務器溝通過程所使用。

依照SMTP協定，退信網域Return-path 等同於寄件人網域MAIL FROM (又名bounce address, reverse path, envelope from, envelope sender, return address)

亦即若有退信，將退到此一網域特定郵件地址，如下圖此一任務發送退信將至 Return.EID44fb8629.Job@mail.neweredm.com，此退信網址為發信機自動產生。



當郵件發送量大或想設定專屬退信網域作為退信，可將此"寄件者"修改成企業本身網域。例如 edm.example123.com，當電子報發送有退信時，就會將退信傳送此網域，對降低退信率有幫助。同時"寄件者"也為企業自有網域，當寄件人網域與寄件者網域兩者一致，也對降低判定成為垃圾信有幫助。

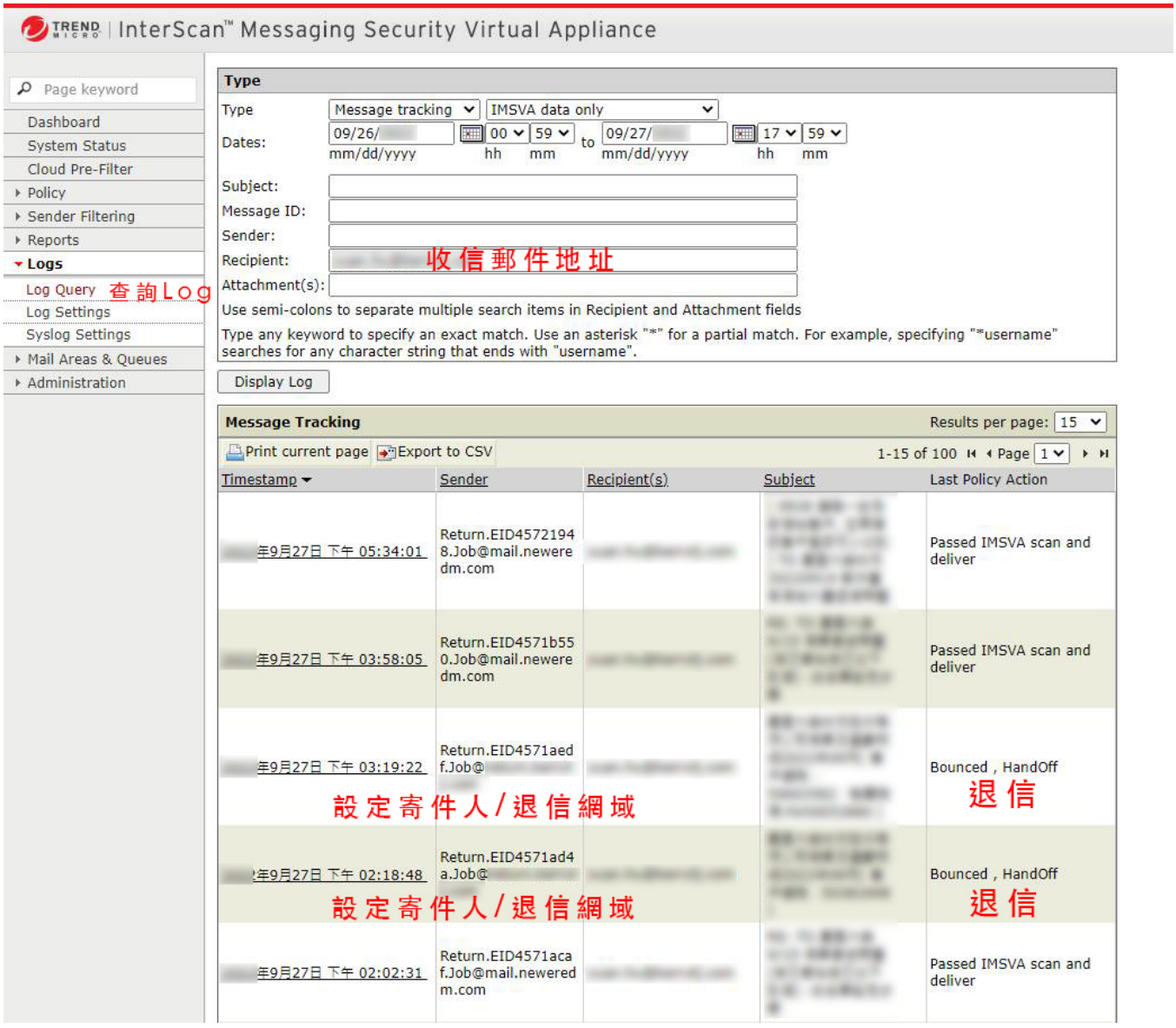
2. 公司內部無法收信

A. 查詢是否郵件被阻擋

公司內部無法收信，最常見原因就是「寄件人」網域與公司網域相同，因此被郵件服務器或是被郵件掃毒/惡意軟體檢查而阻擋。

下圖可看到，原本未設定「寄件人」網域，因此郵件係由《沛盛資訊》發信機網域 mail.neweredm.com 寄出，順利被收信未被阻擋。但當設定寄件人網域，以及與公司自有網域相同，郵件即被阻擋。依照郵件服務器設定不同，也有可能「寄件者」網域與公司網域相同就被阻擋。當確定已經成功發信，且被公司內部郵件服務器接收，檢查是否被阻擋。

若有被阻擋，便要設定例外允許從公司外部由《沛盛資訊》寄送到公司內部網域，該電子報寄件人給予放行。



3. Office 365 寄件與收件同網域放行設定

A. 可參考官方說明。

https://learn.microsoft.com/zh-tw/microsoft-365/security/office-365-security/anti-spoofing-protection?view=o365-worldwide
被稱為「自家人詐騙」，寄件人與收件人同網域(或子網域)

B. Office 365 設定

持有 Tenant 全域管理權限 登入 Microsoft admin center 安全管理中心
(註: Office 365 區分為不同權限版本，需購買足夠高權限版本才能調整)
圖 1

圖 2

圖 3

圖 4

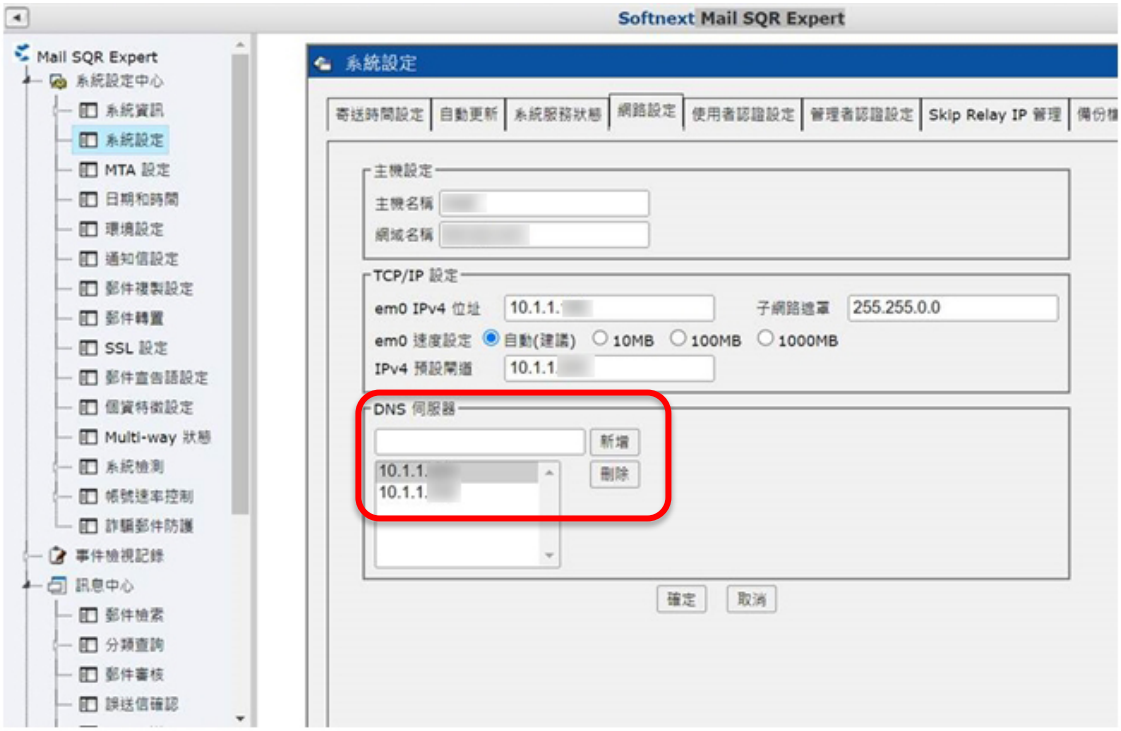
收件者將自己網域[edm@example.com] 加入允許網域

圖 5

2. 中華數位 (Mail SQR Expert) 寄件與收件同網域放行設定

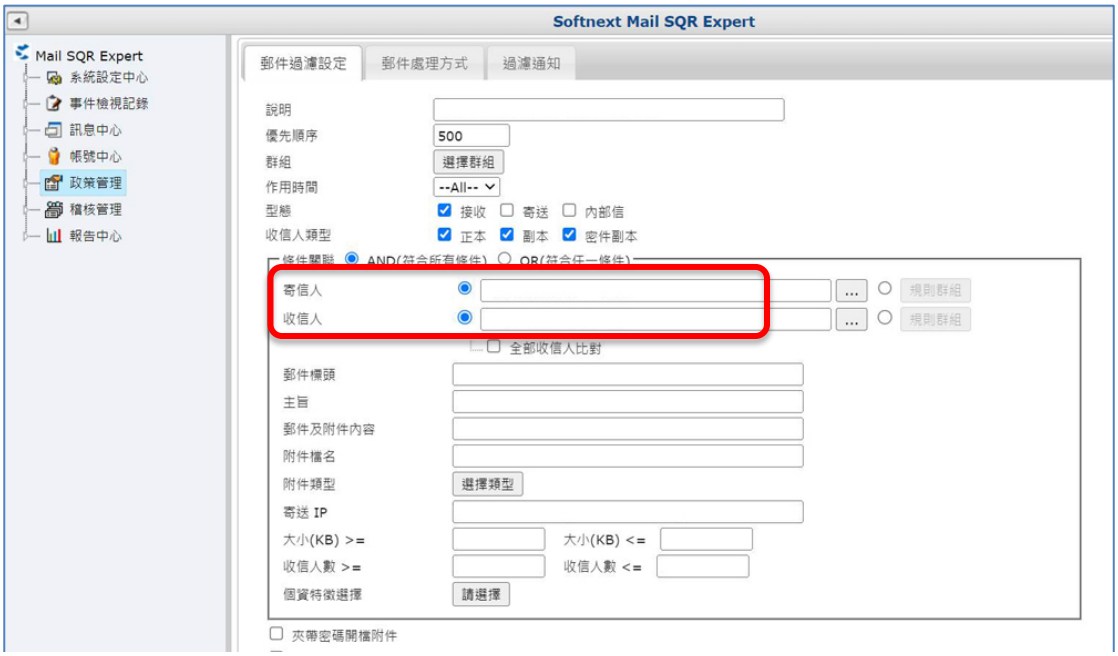
A. 將寄件者網域加入 DNS

將寄件者(退信)網域加入 DNS 伺服器



B. 設定白名單

若設定完 DNS 後仍無法收到，另可在「政策管理」設定中，將電子報寄件人設定為允許派送。



3. 趨勢科技 InterScan (IMSVA) 寄件與收件同網域放行設定

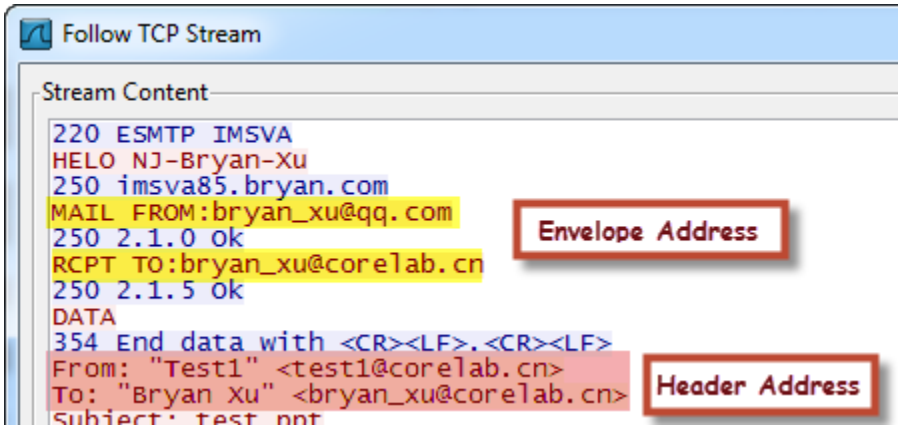
可依趨勢科技 IMSVA 使用手冊進行設定。(以下來源為趨勢科技)

Enhanced Anti-Spoofing Feature

IMSVA contains Anti-Spoofing filter, it can detects and taks action on a message that has the sender domain that is the same as the recipient(s) domain, and the message does not come from an internal IP address.

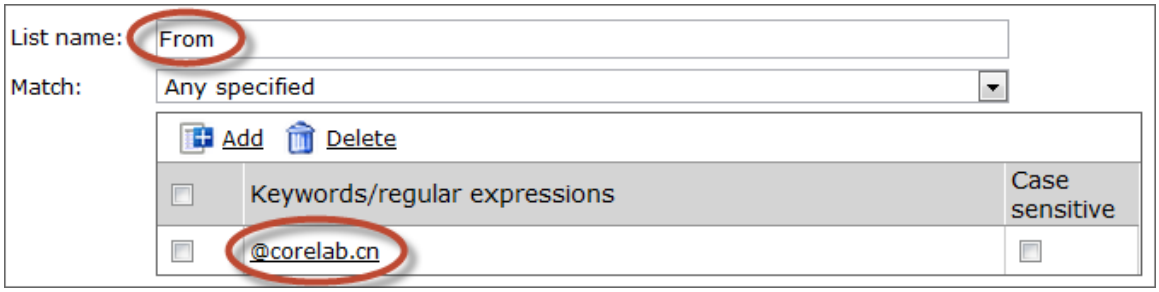
This will only check envelope address.

In order to check both envelope address and mail header address as following chart, administror can create a rule to check both anti-spoofing filter and mail header address.

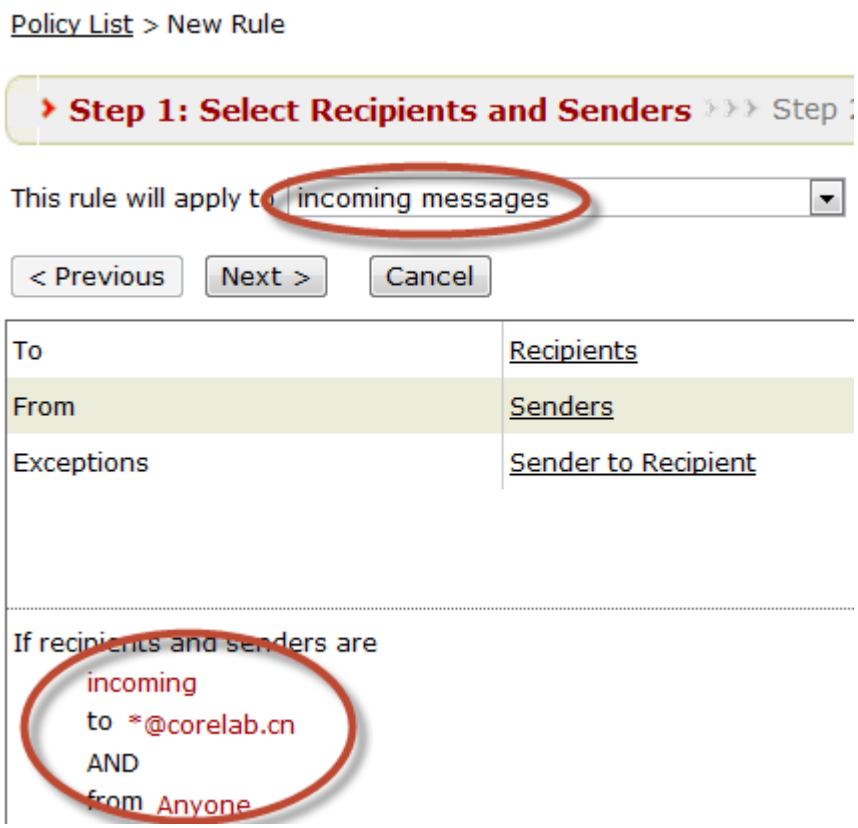


Assume domain is corelab.cn, the related rule could be set as below:

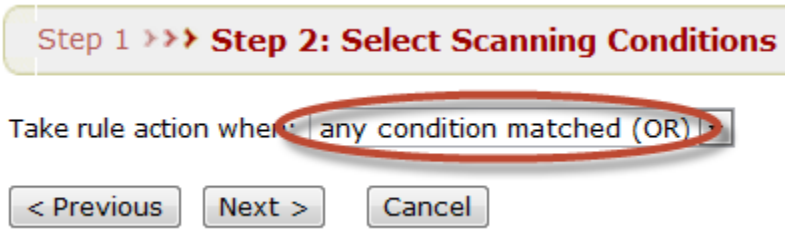
1. Click Plicy → Keywords & Expression, and create a new keyword expression "From" as below:

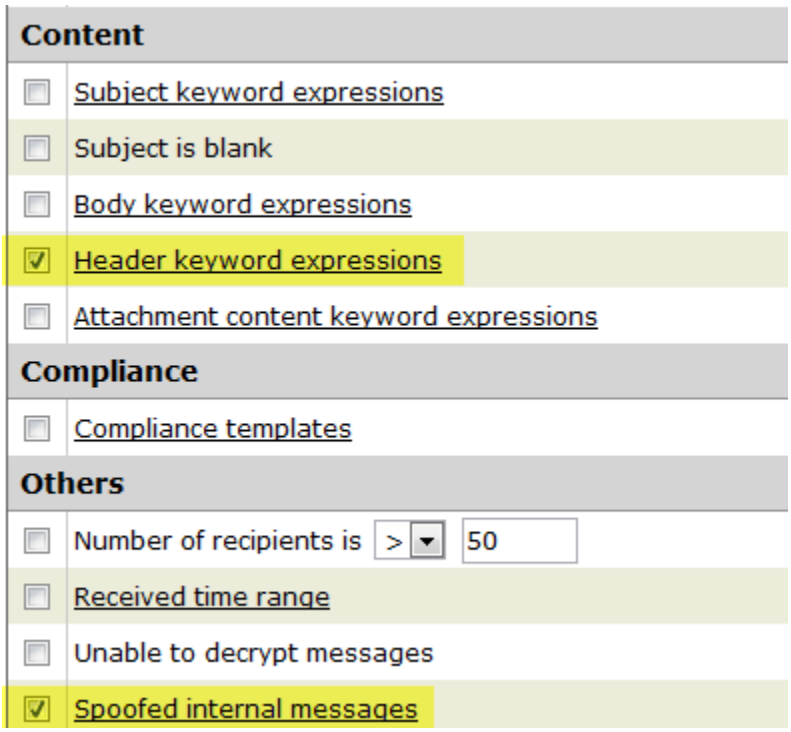


2. Create a new incoming rule (Other type), from **Anyone** to ***@corelab.cn**;

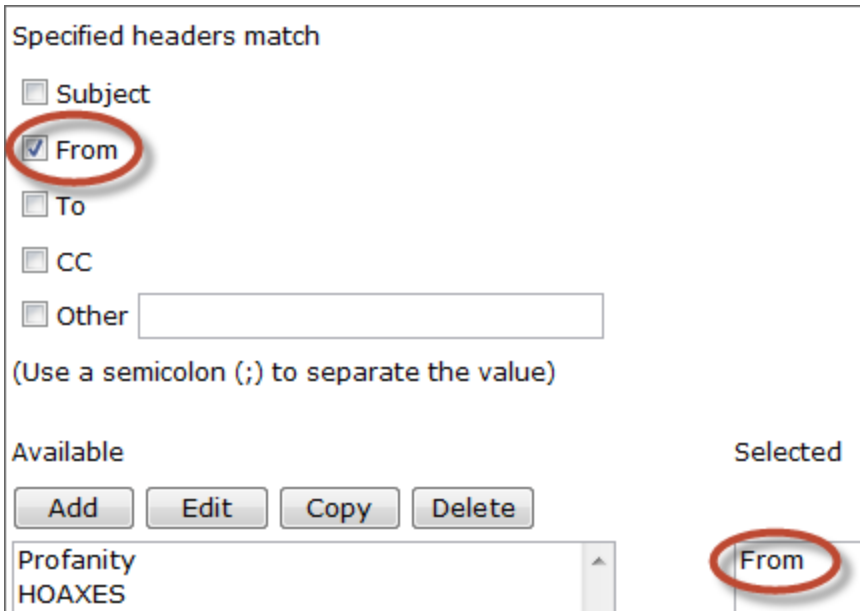


3. For Scanning Conditions, use default "any condition matched (OR)", and select "**Header keyword expressions**" & "**Spoofed internal messages**" filter.





4. For "Header keyword expressions" filter, check **From** header, and use the keyword expression "**From**" that created in Step 1.



1. For "Spoofed internal messages" filter, set the **Trusted Internal IP**, we usually need to add mail server IP as Trusted Internal IP. IMSVA will not checking the mails from listed IP addresses.
2. Set the action as want, such as quarantine the mail.

3. Set the rule name & rule order number, such as set rule name "Anti Spoofing Rule". Rule summary info as below chart:

1. Doing some testing to make sure this rule works fine.

- Insert disclaimer for outgoing email messages

Email disclaimer usually been practiced as a standard in corporate email messaging systems.

Administrators can generate disclaimer referring to following steps.

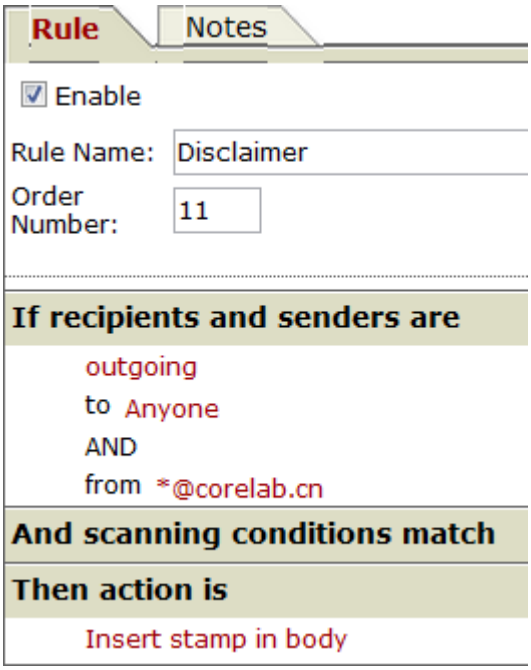
1.1. On IMSVA web console, click Policy → Stamps, add a "Disclaimer" stamp.

1.2. Click Policy → Policy List, add a new outgoing rule (other type), from internal domain to anyone.

1.3. Leave blank for "Scanning Conditions" setting.

1.4. For "Action" part, select "Do not intercept messages" and "Insert stamp in body", and use "Disclaimer" as stamp.

2. Save the rule with name "Disclaimer". Rule summary info as below chart:



3. Doing some testing to make sure the rule works fine.