

---

# 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>

itpison.com. © All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the prior written consent of the publisher. All company and product names are trademarks or registered trademarks of their respective owners.

## TABLE OF CONTENTS

1. 寄件者與寄件人 .....	3
A. 寄件者與寄件人差別.....	3
2. 公司內部無法收信 .....	4
A. 查詢是否郵件被阻擋.....	4
3. Office 365 寄件與收件同網域放行設定.....	5
A. 可參考官方說明 。 .....	5
B. Office 365 設定 .....	5
2. 中華數位 (Mail SQR Expert) 寄件與收件同網域放行設定 .....	7
A. 將寄件者網域加入 DNS.....	7
B. 設定白名單.....	7
3. 趨勢科技 InterScan (IMSVA) 寄件與收件同網域放行設定 .....	8

## 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。

```
ARC-Authentication-Results: i=1; mx.google.com;
dkim=pass header.i=@寄件者網域.com header.s=s1024 header.b=Ku4KVjH+;
spf=pass (google.com: domain of return.eid44fb8629.job@mail.neweredm.com
designates 61.218.78.239 as permitted sender)
smtp.mailfrom=Return.EID44fb8629.Job@mail.neweredm.com; 寄件者網域
dmarc=pass (p=NONE sp=NONE dis=NONE) header.from= [REDACTED].com
Return-Path: <Return.EID44fb8629.Job@mail.neweredm.com>
Received: from b239.neweredm.com (b239.neweredm.com. [61.218.78.239])
by mx.google.com with ESMTPS id p35-
```

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](mailto: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。

The screenshot shows the Trend Micro InterScan Messaging Security Virtual Appliance interface. On the left, there's a navigation menu with options like Dashboard, System Status, Cloud Pre-Filter, Policy, Sender Filtering, Reports, and Logs. Under Logs, there's a red-highlighted link 'Log Query 檢詢 Log'. Below the menu is a search form with fields for Type (Message tracking), Dates (09/26/2018 00:59 to 09/27/2018 17:59), Subject, Message ID, Sender, Recipient (highlighted in red), and Attachment(s). A note below says to use semi-colons to separate items and to use an asterisk '\*' for partial matches. The main area shows a table titled 'Message Tracking' with columns: Timestamp, Sender, Recipient(s), Subject, and Last Policy Action. The table contains five rows of data. Red annotations have been added to the 'Recipient(s)' column in the first two rows and the 'Last Policy Action' column in the last three rows. The annotations read: '收信郵件地址' (Recipient address) and '退信' (bounce).

Message Tracking					Results per page: 15
Print current page		Export to CSV		1-15 of 100	
Timestamp	Sender	Recipient(s)	Subject	Last Policy Action	
2018-09-27 17:54:01	Return.EID45721948.Job@mail.neweredm.com	[REDACTED]	[REDACTED]	Passed IMSVA scan and deliver	
2018-09-27 17:54:05	Return.EID4571b550.Job@mail.neweredm.com	[REDACTED]	[REDACTED]	Passed IMSVA scan and deliver	
2018-09-27 17:54:22	Return.EID4571aedf.Job@	[REDACTED]	[REDACTED]	Bounced , HandOff	退信
2018-09-27 17:54:48	Return.EID4571ad4a.Job@	[REDACTED]	[REDACTED]	Bounced , HandOff	退信
2018-09-27 17:55:31	Return.EID4571acaJob@mail.neweredm.com	[REDACTED]	[REDACTED]	Passed IMSVA scan and deliver	

### 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

A screenshot of the Microsoft Admin Center's 'Principles &amp; Rules' section. On the left, there is a sidebar with various categories like '装置', '端點', '電子郵件與共同作業', etc., and '原則與規則' is highlighted with a green oval. The main content area is titled '原則與規則' and contains a table with columns for '名稱' (Name) and other options. The first row, '威脅原則', is also highlighted with a green oval.

圖 3

## 威脅原則

樣板化原則

	預設安全性原則	透過使用建議的保護範本一次套用所有原則以輕鬆設定保護
	設定分析器	識別您目前原則設定中的問題，以改善安全性

原則

	防網路釣魚	保護使用者免受網路釣魚攻擊，並設定可疑郵件的安全提示。
	反垃圾郵件	保護貴組織的電子郵件免於垃圾郵件的危害，包括偵測到垃圾郵件時要採取的動作
	反惡意程式碼	保護貴組織的電子郵件免於惡意程式碼的危害，包括偵測到惡意程式碼時要採取的動作及要通知的對象
	安全附件	<small>進階版</small> 保護您的組織免於 SharePoint、OneDrive 與 Teams 中之電子郵件附件和檔案所含之惡意內容的危害
	安全連結	<small>進階版</small> 保護使用者免於開啟及共用電子郵件訊息與 Office 應用程式所含之惡意連結的危害

圖 4

收件者將自己網域[edm@example.com] 加入允許網域

原則與規則 > 威脅原則 > 反垃圾郵件原則

## 反垃圾郵件原則

我們建議啟用預先設定的安全性原則，以使用新的安全性控制項和我們建議的設定來保持最新狀態。檢視預設使用此頁面來設定包含在反垃圾郵件保護的原則。這些原則包含連線篩選、垃圾郵件篩選、以及輸出

+ 建立原則 ▾ 重新整理

名稱	狀態
<input checked="" type="checkbox"/> 反垃圾郵件輸入原則 (預設)	一律開啟
<input type="checkbox"/> 連線篩選原則 (預設)	一律開啟
<input type="checkbox"/> 反垃圾郵件輸出原則 (預設)	一律開啟

反垃圾郵件輸入原則 (預設)  
● 一律開啟 | 優先順序 最低

針對網路釣魚郵件啟用  
● 啟動

在此天數內保留隔離的垃圾郵件  
30

編輯動作

允許和封鎖的寄件者和網域

允許的寄件者

-

允許的網域

1 個網域

封鎖的寄件者

-

封鎖的網域

-

[編輯允許和封鎖的寄件者和網域](#)

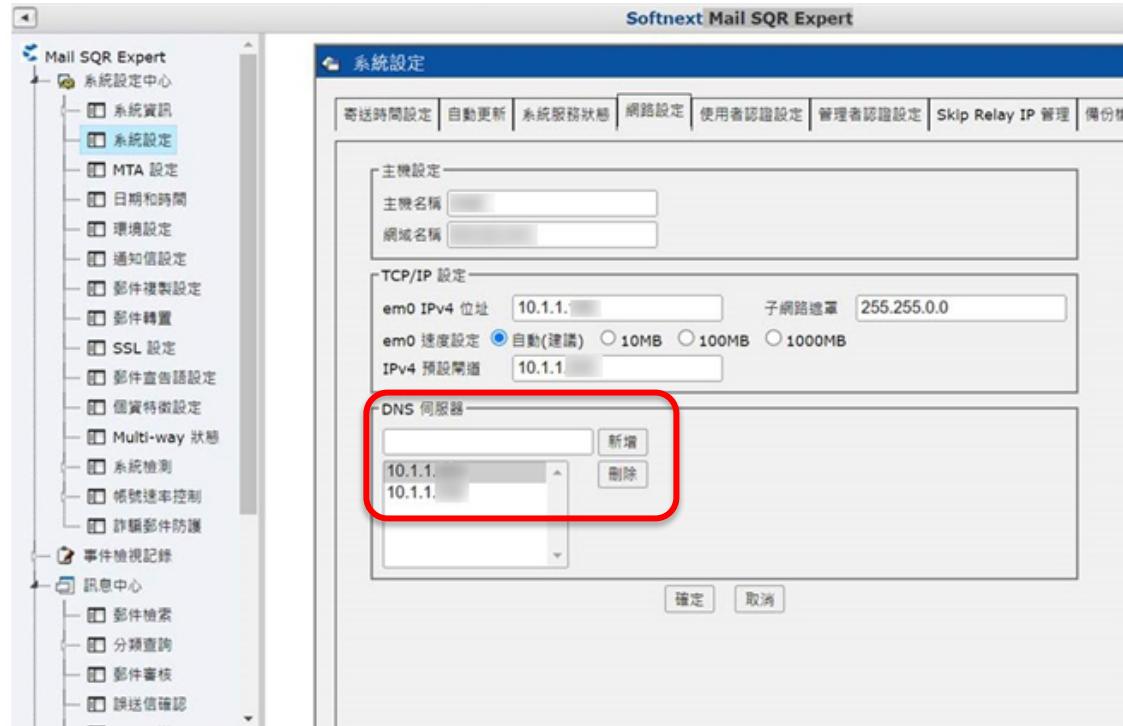
[關閉](#)

圖 5

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

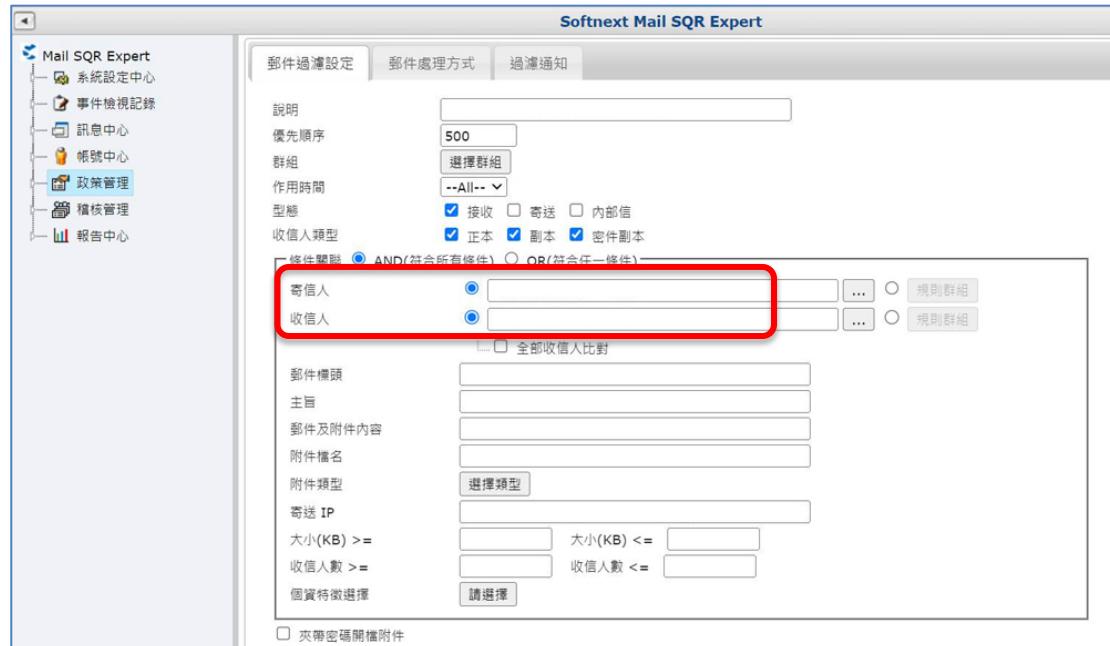
### A. 將寄件者網域加入 DNS

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，將電子郵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 detect and take 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, administrator can create a rule to check both anti-spoofing filter and mail header address.

```
220 ESMTP IMSVA
HELO NJ-Bryan-Xu
250 imsva85.bryan.com
MAIL FROM:bryan_xu@qq.com
250 2.1.0 ok
RCPT TO:bryan_xu@corelab.cn
250 2.1.5 ok
DATA
354 End data with <CR><LF>.<CR><LF>
From: "Test1" <test1@corelab.cn>
To: "Bryan Xu" <bryan_xu@corelab.cn>
Subject: test nnt
```

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

1. Click Policy → Keywords & Expression, and create a new keyword expression “From” as below:

<input type="checkbox"/>	Keywords/regular expressions	Case sensitive
<input checked="" type="checkbox"/>	@corelab.cn	<input type="checkbox"/>

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

[Policy List](#) > New Rule**Step 1: Select Recipients and Senders** >>> Step 2This rule will apply to **incoming messages**

&lt; Previous

Next &gt;

Cancel

To	<a href="#">Recipients</a>
From	<a href="#">Senders</a>
Exceptions	<a href="#">Sender to Recipient</a>
<hr/>	
<b>If recipients and senders are</b>	
<b>incoming</b>	
<b>to *@corelab.cn</b>	
<b>AND</b>	
<b>from Anyone</b>	

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

**Step 1 >>> Step 2: Select Scanning Conditions**Take rule action when **any condition matched (OR)**

&lt; Previous

Next &gt;

Cancel

**Content**

- [Subject keyword expressions](#)
- [Subject is blank](#)
- [Body keyword expressions](#)
- [Header keyword expressions](#)
- [Attachment content keyword expressions](#)

**Compliance**

- [Compliance templates](#)

**Others**

- Number of recipients is >
- [Received time range](#)
- [Unable to decrypt messages](#)
- [Spoofed internal messages](#)

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

Specified headers match

- Subject
- From
- To
- CC
- Other

(Use a semicolon (;) to separate the value)

Available	Selected
<b>Add</b> <b>Edit</b> <b>Copy</b> <b>Delete</b>	<b>From</b>
Profanity HOAXES	

- 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.
- 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:

[Policy List](#) > [Rule Summary](#)

[Save](#) [Cancel](#)

Rule	Notes
<input checked="" type="checkbox"/> Enable	
Rule Name:	Anti Spoofing Rule
Order Number:	10
<b>If recipients and senders are</b>	
incoming	
to *@corelab.cn	
AND	
from Anyone	
<b>And scanning conditions match</b>	
Specified Header matches ...	
OR	
Spoofed internal messages	
<b>Then action is</b>	
Quarantine message	

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:

Rule	Notes
<input checked="" type="checkbox"/> Enable	
Rule Name:	Disclaimer
Order Number:	11
<b>If recipients and senders are</b>	
outgoing	
to Anyone	
AND	
from *@corelab.cn	
<b>And scanning conditions match</b>	
<b>Then action is</b>	
Insert stamp in body	

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