建置防毒與防垃圾信系統之測試環境

實驗手冊

Ⅰ. 實驗目的

電腦病毒及最近興起的惡意程式對日趨複雜的網路使用環境造成極大的威脅，從早期的紅色警戒、ＣＩＨ等等對使用者造成極大傷害的病毒，到近期鑽微軟作業系統漏洞的ＭＳＮ病毒、疾風病毒等，都可能對用戶及企業的資料造成極大的損傷。也因此，瞭解病毒的特性以架構一個可以偵測病毒的安全環境就成了本實驗的重點。

此外，在資料流通的世界中，垃圾郵件的產生不但造成閱信者使用上之耗時及不便，更時常造成網路頻寬之浪費及加重網路設備之承載，根據統計，全球垃圾郵件約佔總郵件量的 75%～82%，每年造成網路服務商五億美元的浪費。更有甚者，垃圾郵件進而成爲網路釣魚(Phishing)等犯罪手法的溫床，因此本實驗亦對垃圾郵件的問題加以探討。

綜合以上兩點，本實驗之目的有三：

1. 熟悉垃圾郵件的特性以及待測物規格，進而建置正確的功能測試環境。
2. 瞭解病毒在各種通訊協定上流通的方式以及待測物規格，進而建置正確的功能測試環境。
3. 使用 Postal/Rabid 建測效能測試環境。

操作本實驗的同學應具備基本的網路知識，瞭解各種通訊協定的基本意義，以及具備簡單的 Windows 作業系統之操作能力。此外，Postal 的操作亦需要簡單的 Unix-like OS 的操作能力。本實驗範例所使用的待測機器爲 Fortigate 400A，爲一多功能防火牆（防毒／擋垃圾郵件），然本實驗不限定待測機器，同學可以使用手上可得的軟硬體資源來驗證本實驗，常見於測試本實驗的軟體環境有 WinMail 等。

Ⅱ. 實驗設備

硬體

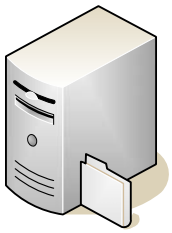
項目	數量	備註
個人電腦	3	一台伺服器及兩台用戶

		端
Router	1	含可設定的防毒及阻擋垃圾信件功能
網路卡	3	
網路線	3	

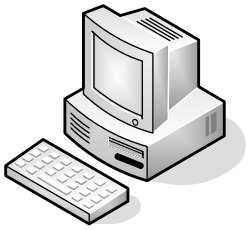
軟體

軟體名稱	數量	軟體種類	描述
Windows XP	1	OS	
Fedora Linux Core 3	1	OS	主要用來跑 Postal
Serv-U	1	FTP Server	
LeapFTP	1	FTP Client	
Apache	1	HTTP Server	
M-Daemon	1	Mail Server	
Postal/Rabid	1	Mail Simulation	

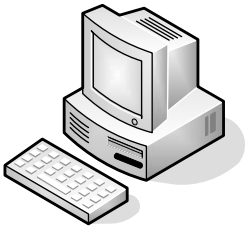
下面爲機器的詳細使用說明，同學可以依照需要自行架設機器或者參考下面的圖示來安裝本實驗所需要的機器以及環境。



Server: 用來當作提供檔案的伺服器，基於實驗需要，我們在此機器上架設FTP Server (Serv-U)、HTTP Server (Apache)、Mail Server (M-Daemon)



Client: 用來作爲實驗中模擬真實世界中用戶端的機器，基於此目的，我們在上面架設可以與Server互相溝通的Client端軟體，如FTP Client (LeapFTP)以及用微軟預設的IE以及Outlook Express等。本機器也於實驗三中充作Spammer使用。



Performance Tester: 本機器特別使用於實驗四，因此測試Server效能時所需要的效能測試軟體Postal/Rabid就安裝在這台機器上，作業系統必須爲Unix-Like的相關OS。

Ⅲ. 背景資料

Anti-Virus(HTTP、FTP、IMAP、POP3、SMTP)

在資訊安全領域中，最常被探討的資訊威脅來源就是病毒及其他各式的新興

惡意程式如木馬及 Attacker 等。一般來說，傳統家用使用者對病毒並沒有一一破解的方法，通常需要依靠防毒廠商的軟硬體支援來達到防毒的目的。傳統廠商對於病毒的防治不外乎在全球各地設定使用者回報系統，然後根據回報的病毒作破解，然後更新病毒碼供使用者更新。較爲消極的硬體防治方法則爲限制使用者下載／接收某些特定型態的檔案，例如執行檔、VB Script、以及容易感染巨集的文件檔等，這種方法最常使用在郵件相關的通訊協定。此外，目前有特定廠商亦提供 Grayware(惡意程式)的偵測，例如 Joke 或者是 Trojan 等的新興入侵方式的防治。最後，所有的病毒都可以藉由壓縮以及加密來僞裝，一個安全的防毒環境必須要能對經過壓縮的文件做檢測，市面上流通的壓縮格式約在二十至三十種之間，許多壓縮檔案甚至標榜可加密的功能，往往成爲網路下載偵測的死角，這點也是一個好的網路管理者所需要考量的技術挑戰。以下便是針對上述各項技術、需求及偵測方法的簡略介紹。

需求	方法	技術應用層次
掃描病毒	對於下載／上傳之文件作病毒碼資料庫之比對	HTTP、FTP、IMAP、POP3、SMTP
擋除不完整之檔案	對於不完整的信件必須有擋除的功能	IMAP、POP3、SMTP
擋除特定格式之檔案	擋除可能危險的附加檔	HTTP、FTP、IMAP、POP3、SMTP
檢查／掃描壓縮檔	對於壓縮檔作解壓縮、並且掃描的動作，一般來說必須支援多層解壓縮的動作	HTTP、FTP、IMAP、POP3、SMTP

表 三之一 電腦病毒防治的基本功能需求

Anti-Spam (IMAP、POP3、SMTP)

垃圾郵件的判定不如病毒容易，病毒的偵測要點不外乎判斷一程式是否會惡意地造成電腦資料損壞或者系統之不穩定，然而垃圾郵件在規格上與一般郵件卻無兩樣，也因此，要如何判定正常郵件與垃圾郵件的差別，便依靠下麵幾項特點的偵測：首先，垃圾郵件通常會大量發信，故可以從區域使用者回報之黑名單或者限制收發信頻率直接將 Spammer 擋除。第二，Spammer 爲了反制用戶對第一點加以限制，便以流動之位置爲 Server 架設之地點，通常爲一未向 DNS 註冊之位置，故可以反查 DNS 以確定使用者來源之真實性。第三，可以依 Spam Mail 中特定字眼或特定檔案類型出現之高頻率的特性來加以擋除，此種技術利用 banned word list 檢查信件內容以判定是否爲垃圾信件，許多廠商利用智慧訓練的機制防止誤判，不失爲一好方法。最後，許多 Server 提供 Relay 之服務，或者是主機被入侵而不知覺中成爲 Relay Server，此時我們也可以檢查 Open Relay

Database 以擋除來自跳板之信件。

下面便是一個好的 Anti-Spam 系統所需要有的基本功能：

須求	方法	技術
已知 Spam 寄信方之 IP 或者 E-mail Address	藉由 filter 將所有來自 Spammer 地址的信件擋除	1. IP address FortiSpamshield 2. IP address BWL 3. E-mail address BWL
利用 Spammer 多爲未向 DNS 註冊之流動位置的特性，擋除來自 Spammer 的信件	反查 DNS，看是否有回應，若無回應則擋除，判定爲非法的垃圾郵件	1. HELO DNS lookup 2. DNSBL 3. Return e-mail DNS check
防止被跳板攻擊之來源	建立 Open Relay Database，反查來源是否爲一 Open Relay Mail Server	1. ORDBL: Open Relay Database Lists 2. RBL: Real-time Blackhole Lists
利用 Spam Mail 常出現特定字眼(如色情與金錢)的特性擋除 Spam	建立 banned word list，擋除含有 banned word 之信件，此部分有多種作法	1. Banned word check
垃圾郵件多帶有圖片或多媒體附加文案，若一信件有特定之 MIME Header，便爲一可疑的信件	檢查 MIME header	1. MIME headers check
垃圾郵件通常會是短時間內大量的出現	檢查來自某網域信件或某特定位址信件的出現頻率	1. Frequency Check
在 SMTP 通訊過程中，有一些郵件地址，如郵件發送者 FROM 地址不符合 RFC822 規定	檢查郵件的 FROM 欄位	1. FROM address check

表 三之二 垃圾郵件之特性與其防治方法／技術

下面我們針對一些比較重要的技術的背景做介紹：

其中檢查 MIME Header 部分主要爲了抑止惡意郵件，當 Exchange Server 進行一般檢查外來電郵的 MIME Header，一些特定類型的無效數值在某些欄位出現會使到 Exchange Server 運作停頓。這就是著名的「不正確的 MIME 檔頭」("Incorrect MIME Header") 系統安全弱點。關於本項可以參考微軟補釘 MS01-020 的說明。

此外，若 Anti-Spam 系統提供者身兼郵件服務提供者，近年來興起的另一個

主動式防止垃圾郵件的技術爲”信箱分身”功能，即在寄信的時候提供使用者將信箱名稱稍做改變(例如在原有的名稱後面增加數字)，避免原始信箱帳號流入 Spammer 手中而成爲垃圾郵件的受害者。

另外亦有較爲嚴謹的方法，即一般廠商會實作的黑名單／白名單機制，黑名單的過濾機制主要是廠商或使用者本身維護一個黑名單資料庫以阻擋某些特定地址及網域的電子郵件，黑名單資料庫維護得當就能夠很有效的遏阻一些已知來源的電子郵件，但也因爲其不是很精細的過濾方式所以很容易連同不必要的電子郵件都一併擋掉(例如會把整個網域的信件一起擋除而不考慮合法非法位址)。也因此從這裡衍生出所謂的白名單機制，白名單管理是非常準確的過濾方式，其蒐集所有允許的電子郵件地址及網域名單，使其可以與企業正常收發名單內的信件，其可與黑名單搭配使用，而行成互補功用，黑名單阻擋一般性的網域而白名單則開放該網域中的某些特定郵件。

而 RBL(Real-time Blackhole Lists) 過濾是當發送郵件時檢查發送郵件來的客戶端或其它郵件服務器的地址是否已被防止垃圾的組織禁止，有許多垃圾郵件的發送大國(如中國)，幾乎全國的主要伺服器都在 List 之內，若要接收來自這些國家的信件，則必須關閉此項。

最後我們討論一種最重要的機制，也就是 DNS 反查(DNS Lookup)以及 HELO DNS 反查，這種方式是針對傳送至企業的電子郵件之 IP 位址以反查的方式，來確認出傳送郵件的主機名稱，因爲很多的垃圾郵件會利用假借的主機名稱來傳遞郵件以隱藏其真實來源。所以在 DNS 反查的方式就會將系統無法找到合法的主機及 IP 位址之信件判斷爲垃圾郵件。

而檢查 HELO/EHLO 的主機名主要是在 SMTP 通訊過程中，發送端會發送 HELO/EHLO 命令，標準的協定中是跟隨主機名或域名，可以直接過濾主機名和檢查 HELO/EHLO 主機名的 A 記錄或 MX 記錄與連接的 IP 地址是否匹配。這樣亦能有效的過濾垃圾郵件。

Postal/Rabid(POP3、SMTP)

在一般的 SMTP/POP3 Server 效能測試中，如何快速的產生大量的郵件資料一向是測試人員所關注的部份，傳統硬體支援的做法如 SmartBits/Avalanche 可以快速且大量地產生郵件資料，但是其所費不貲，並非所有的測試人員皆可使用。較爲省錢的解決方法最有名的則有純軟體的 Postal(SMTP)/Rabid(POP3)。這套軟體本來設計的目的在於測試 SMTP Server，後來發展出測試 POP Server 的 Rabid，兩者組合起來便成了今日測試郵件伺服器時常用的 Postal/Rabid Suite。這套軟體最著名的特色是可以根據使用者所提供的郵件帳號列表，自動產生可能的隨機變換以得到大量的 TO-FROM 位址。如同 SmartBits/Avalanche，這套軟體也提供頻寬限制的功能，讓測試者可以限制每分鐘傳輸的郵件數與連線數，這個功能最主要的目的還是在於讓使用者可以根據自己機器的等級來調整軟體。這套軟體會根據上述位置送出隨機資料(信件內容與主旨皆爲隨機產生資料)，然而爲了避免成

爲攻擊工具，Postal 會在信件加上 X-Postal 的檔頭，伺服器管理者可以輕易的對這個檔頭做過濾以避免有心人士的攻擊。最後，這套軟體可以搭配效能測試工具，讓使用者測知網路傳輸的瓶頸，需要注意的是，若使用者需要測試此項目，可將 Postal/Rabid 的極限速度(maximum-speed)設成機器極限速度的一半，以避免效能測試工具對機器的 Bottleneck 造成影響。

Ⅳ. 實驗方法

本實驗的目的在於使同學瞭解病毒以及垃圾信件的性質以架構一個可以偵測病毒與垃圾郵件的環境。本實驗操作環境可在可以直接連接(一般校園網路環境)Internet 的實驗室中進行。利用HTTP Server/Client、FTP Server/Client、以及Postal/Rabid (Performance)跟Mail Server/Client (Functionality)架構一個接近真實世界的環境。再利用所提供的Anti-Virus/Anti-Spam Firewall來設定防毒及防堵垃圾郵件的功能。

爲了模擬真實世界的環境，本實驗分成以下四個階段：

第一個階段模擬LAN的環境。安裝一台Server及一台Client，並設定Firewall監控流通期間的流量。爲確保流量經過防火牆，我們必須確定在Client與Server之間沒有遺漏的路徑，接著就可以開始第二階段以後的測試。

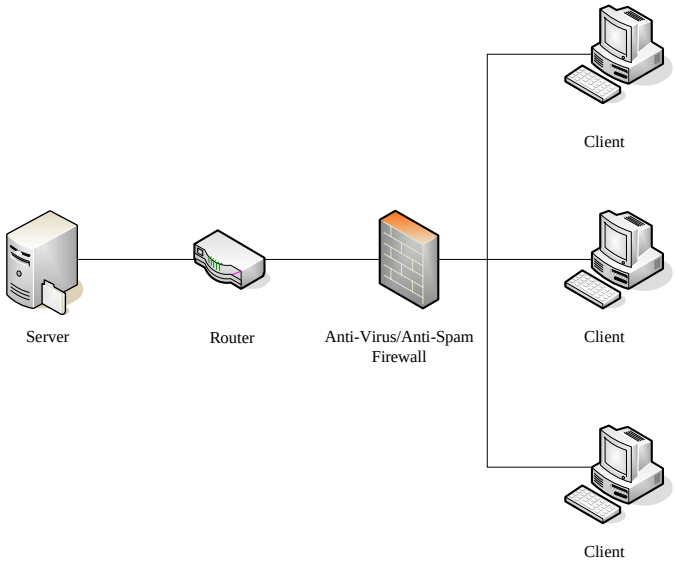


圖 五之一 本實驗第一階段之架構

第二個階段了解病毒的特性，設定Firewall阻擋來自各種通訊協定的病毒及可疑檔案，我們必須在Server上架設各式的Service來提供Client連接。此外，Fireawall對檢查壓縮檔案的支援亦在我們的考量之中。因此首先我們架設FTP/HTTP/SMTP/POP3的伺服器各一台(若機器不足亦可架設在同一台機器上)，讓終端使用者下載或上傳檔案，在實驗過程中設定防火牆以確定資訊環境

的安全，並透過防火牆之紀錄檔來驗證實驗的正確性。

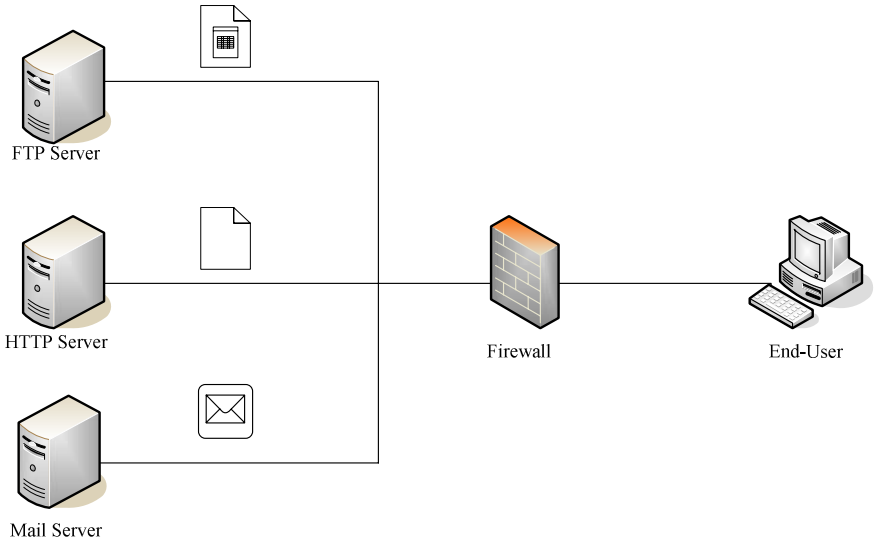


圖 五之二 本實驗第二階段之架構

第三個階段了解垃圾郵件的特性，練習設定Firewall阻擋各種可能的垃圾郵件，包括大量發送，可疑來源郵件，Pattern郵件等，儘可能地利用已知的功能來防堵各式各樣的垃圾郵件。我們在Mail Server端產生各式各樣可能的垃圾郵件(包括使用垃圾郵件常見的Banned Word Pattern以及對使用者端大量發送郵件等)來測試本實驗的正確性。

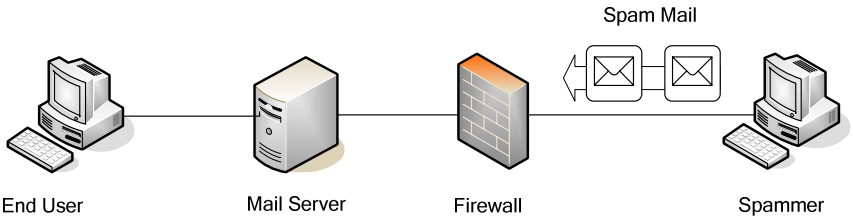


圖 五之三 本實驗第三階段之架構

第四個階段必須開始測試Firewall運行的效能，我們必須在一台Unix-like的機器上面架設Postal/Rabid，隨機產生測試郵件檔，並且觀察Client/Server間的防火牆的運作情形。

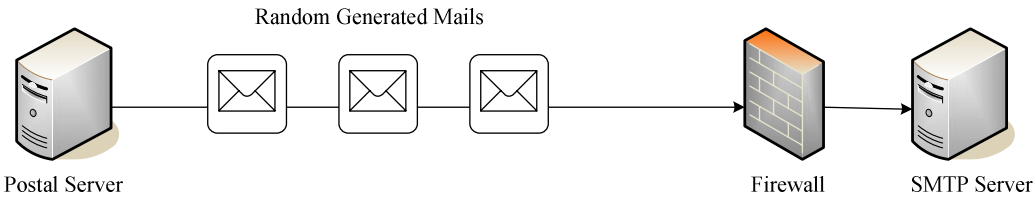


圖 五之四 本實驗第四階段之架構

第四個實驗中，Postal 較爲重要的參數意義如下：

smtp-server: 欲測試的 SMTP Server 之 IP Address，若所設的 Port 不是預設的 25，則可以使用 *ip_address[port]* 的寫法來表示。

user-list-filename: 包含要送達 SMTP Server 上的信件的 username，爲求保險可以完整的寫出全稱的格式，例如：*username@server_address*。這裡要注意的是，username 必須是 SMTP Server 可辨識的名稱，通常我們直接使用 SMTP Server 上的帳號。

conversion-filename: 可選可不選的選項，對 user-list(即上項)做指定的名稱轉換，詳細的轉換規格爲 regular-expression，可以查詢 postal 的使用手冊。

p [processes]: 指定 postal 用來連線的 process 數目。

messages-per-connection: 每個 SMTP 所送的郵件數目。

max-messages-per-minute: 每分鐘能送出的最大郵件數目。

其餘參數在本次實驗中未使用，若有興趣的同學可以參考 postal 的使用說明，其中有許多在現實世界中有用的參數(例如 SSL，用以測試支援 SSL 的 SMTP Server)。

下面列出本次實驗中未使用的參數意義:

local-address: 決定哪個本端 IP 位址要作爲對外連線的 IP。

a: 開啓所有記錄(logging)的選項。

b: 在 Netscape 的 Mail Server 上，軟體會自動將郵件標題開頭多餘的空白(space)去除，這個選項決定是否在標題前方加上空白(space)，-b netscape 會避免加上空白，以免造成 Netscape Mail Server 處理錯誤的機率，-b nonnetscape 則永遠會在標題加上空白，可以用來測試 Netscape Mail Server 以及其他類的 Server 對於此類信件的處理正確性。

s: 決定使用 SSL 連線的百分比，0 是不使用 SSL，100 是總是使用 SSL 連線。

z: 讓使用者分別針對每個 thread 分配一個偵錯檔(debugging file base)，此偵錯檔會記錄每個 thread 的 I/O 動作

Z: 和 z 的意義差不多，爲一的差別在於它會針對每個連線(connection)做紀錄。

Rabid 的參數說明則大致與 postal 相同，只是測試的是 POP Server，爲一個從 POP Server 接收郵件的測試程式。Rabid 的 User-list-filename 格式爲 *username@server_address password* 這是考慮到 POP3 通訊協定必須使用 username 與 password 所做的考量。

下面列出 Rabid 跟 Postal 不同的參數:

i: IMAP 連線的百分比例。(預設爲全部都是 POP 連線。)

b: Qmail POP Server 會在其上的信件結尾加上一行多餘的空白行，-b qmail-pop 意指不要將這樣的信件回報成錯誤信件(error)。

d: 下載比例。這個選項決定有多少郵件會被下載而多少郵件會被刪除。

Postal 目前仍然在開發階段，對於 Postal 開發情形有興趣的同學可以參考 Postal 的官方網站：

http://www.coker.com.au/postal/

由於 Postal 是著名的開放原碼程式，同學們也可以到 SourceForge 網址查看這個程式的開發進度、mailing list、以及相關的資源。

http://sourceforge.net/projects/postal/

V. 實驗步驟

在開始實驗之前，我們假設您已經大致熟悉 Windows 的基本操作，並且瞭解 Windows 下網路的設定，會架構簡單的區域網路(LAN)系統，以及大致瞭解各種通訊協定的 Client(例如 HTTP 下麵的瀏覽器、FTP 下的 Client)如何操作。

第一階段實驗，如圖五之一，設定 Firewall 使其監測由外往內的通訊。首先我們先架設一台 Windows XP 做爲外部伺服器，經過 Router 之後再進入內部網路，中間便是 Firewall 監視通訊。首先設定 Router 及 Client/Server 使其爲同一網域，確定網路的流向強制爲 Server ⟷ Firewall ⟷ Clients。設定完成後，使用 Client 機器測試，並且檢查 Firewall 上面流量之 log，確定設定正確。

第二階段實驗，著重在防火牆於防毒功能上的測試，下面是本階段實驗中該著重的部份：

	測試項目
防毒功能測試／驗證	1. 支援的通訊協定 2. 防毒率 3. 支援的壓縮格式 4. Clean 功能的支援 5. 支援多層壓縮檔的掃毒 6. 多檔傳輸時是否會留下健康檔案而檔除病毒檔？ 7. 對於單一通訊協定是否支援多 Port 的監測

下面我們將一步一步介紹上述七個步驟的詳細實驗方法

1. 支援的通訊協定：
   甲、首先我們將 Client 與 Server 設定在兩個不同的子網域，並且在其間架設防火牆。確定防火牆可以監測到兩個不同子網域之間的流量。
   乙、在 Server 端架設 HTTP、FTP 以及 Mail(含 SMTP 與 POP3 通訊協定) Server。
   丙、開啓防火牆設定介面，確定防火牆未擋除上述四種服務。
   丁、在 Protection Profile 部份，將上述四種通訊協定服務的防毒部分開啓。

戊、接下來開始測試各通訊協定。

i. 首先 Client 從 Server 透過 HTTP 通訊協定下載病毒檔案。通常是從一個架設的網頁下載病毒檔案。
ii. Client 透過 Server 的 FTP 通訊協定下載病毒檔案。
iii. 利用 Client 端的郵件軟體，往 Server 端寄出信件，信件中夾帶病毒檔案，測試 SMTP 協定下的防毒功能。
iv. 利用 Client 端的郵件軟體從 Mail Server 上收病毒信，測試 POP3 協定下的防毒功能。

2. 防毒率：

甲、首先在 Server 端放置大量，具公信力的病毒檔案。
乙、設定防火牆，將 FTP 通訊協定下的防毒開啓。
丙、利用 FTP 通訊協定，從 Server 端下載所有病毒檔案，觀察防火牆上的 log 檔案，計算防火牆的防毒率（擋除檔案／全部檔案）。

3. 支援的壓縮格式：

甲、首先將一隻防火牆可辨識的病毒檔案以各種壓縮格式壓縮(壓縮格式見表六之三)。
乙、設定防火牆，將 FTP 通訊協定下的防毒開啓。
丙、透過 FTP 通訊協定，下載此病毒的各種壓縮格式檔案，紀錄支援的格式。

4. Clean 功能的支援：在病毒壓縮檔掃描的過程中，若壓縮檔中包含健康檔案與病毒檔案,則我們定義 clean 這種清除方式如下:clean 的定義: 接收、(解壓縮)、清除病毒檔、(壓縮)、送出。我們測試以下列方式測試本子項：

甲、將病毒檔案與健康檔案混合，壓縮（請以防火牆支援的壓縮格式壓縮）成單一個壓縮檔案。
乙、設定防火牆，將 FTP 通訊協定下的防毒開啓。
丙、透過 FTP 以及 POP3 通訊協定，下載此壓縮檔案。
丁、若下載成功，檢查下載回來的壓縮檔案是否與原檔一致？
戊、若下載不成功，檢查防火牆的 log，紀錄防火牆對於此種檔案的動作。

5. 多層壓縮檔的掃毒支援：

甲、首先將選取一隻防火牆可辨識的病毒檔案。
乙、將上述病毒利用防火牆支援的壓縮格式反覆壓縮，分別壓縮兩次，五次，十次，五十次，得出數個壓縮檔案。
丙、設定防火牆，將 FTP 通訊協定下的防毒開啓。
丁、透過 FTP 通訊協定下載上述多層壓縮檔案，若支援多層壓縮檔的掃毒，紀錄支援的層數。若不支援，觀察防火牆的 log 檔案，紀錄防火牆對此種檔案的處理方式。

6. 多檔傳輸時是否會留下健康檔案而檔除病毒檔：某些廠商對於掃毒的過程較爲嚴苛，若一個 session 中（例如 FTP Session）偵測到一個病毒檔案，便將整個 session 給檔除(block)。甚至同一機器會對不同的通訊協定有不同的處理方式。依照下述步驟檢測您所測試的防火牆：

甲、首先準備多個病毒檔案與多個健康檔案，下麵是各種通訊協定下的測試方式：

i. HTTP：Client 從 Server 的下載網頁交互下載病毒與健康資料，觀察是否可以在防火牆偵測到病毒檔之後,從同一網頁下載健康資料？
ii. FTP：將病毒檔案與健康檔案混合命名，利用 FTP Client 端下載軟體批次下載，觀察是否可以在防火牆偵測到病毒檔之後，在同一個 session 繼續下載健康檔案？
iii. SMTP：往 Server 端批次寄出多封信件，其中包括夾帶病毒的信件與夾帶健康檔案的信件,觀察是否可以在防火牆偵測到病毒檔之後，無礙地繼續寄出健康郵件。
iv. POP3：從 Server 接收多封信件，其中包括夾帶病毒的信件與夾帶健康檔案的信件,觀察是否可以在防火牆偵測到病毒檔之後，無礙地繼續接收健康郵件。

7. 對於單一通訊協定是否支援多 Port 的監測：傳統的防火牆通常對於某些標準的通訊協定僅支援預設 Port 的監測(例如：FTP 的 21 埠，HTTP

的 80 埠等)，但是各種通訊協定下的 Server 應用程式多可支援更改預設埠的功能，我們藉由 FTP Server 軟體來驗證防火牆是否支援多埠的監測。

甲、首先設定一 Server 端的 FTP 伺服器軟體，將 Port 改爲 2100，再將另一 Server 端的 FTP 伺服器軟體的 Port 改爲 210。

乙、設定防火牆，將 FTP 通訊協定下的防毒開啓。

丙、Client 端分別從兩台 Server 端接收病毒檔案，觀察防火牆是否正確擋除病毒檔案。

第三階段實驗，著重在找出垃圾郵件與一般郵件的不同之處，利用垃圾郵件的特性設定防火牆以達到防堵垃圾郵件的效果，下面就是本次實驗中我們所著眼的部份：

	測試項目
阻擋垃圾郵件功能測試／驗證	1. 反查 DNS，驗證是否爲合法位址 (DNS Lookup／HELO DNS Lookup) 2. 直接阻擋特定來源位址的信件或阻擋來自特定網域的信件(黑名單過濾)以及永遠允許特定郵件通過(白名單過濾) 3. 擋除含特定字眼的信件 4. 限制發信頻率

下麵我們便一步一步說明各項測試的詳細步驟：

1. 我們將 Spammer 的位址移到不合法的網域(即不爲 End-User 及防火牆的 DNS 所解析的位址，通常是一浮動位址)，從 Spammer 往 End-User 寄信，觀察 End-User 是否能收到來自 Spammer 的信件？
2. 在測試機器的 Spam Filter 選項的 IP Address Filter 中增加 Spammer 機器的 IP Address，接著從 Spammer 往 Server 寄出信件，觀察 End User 是否能收到信件？
3. 在測試機器 Spam Filter 選項的 Banned Word 項目中增加一個 Banned Word(例如：Sex 或者 Drug)，接著從 Spammer 機器往 Server 寄出含有 Banned Word 的信，觀察是否能從 End User 端正確的收到原始信件？
4. 我們在此階段必須設定防火牆所能容忍的郵件頻率，藉由固定此頻率，我們調整 Spammer 的寄信頻率，觀察 End-User 是否能夠接收到來自 Spammer 的信件

第四階段實驗，如圖五之四，首先我們先將最新版的 Postal(本例中爲 0.62 版)下載至我們要安裝 Postal 的 Linux／Unix Server 上面，使用 tar 解壓縮之後接著下以下參數：

./configure install　(注意，postal 需在有 GCC/G++之機器上完成安裝)

之後便可以在機器同一目錄下看到 postal，rabid 以及 postal-list 三支程式。

接著便敘述本階段實驗的主要目的：

	測試項目
效能測試／驗證	1. 修改 Postal 各項參數，測試 SMTP 伺服器

	效能 2. 修改 Rabid 各項參數，測試 POP 伺服器

在效能的測試中有一些重要的參數會大大影響待測機器的總體處理能力，像是同時進行的 Process 數目(參數 –process)、限定每分鐘至多能送出多少郵件 (參數 max-messages-per-minute)、郵件大小(maximum-message-size)等，本實驗的目的就在於藉由調整出最適宜的參數，觀察待測物的效能上限，並且瞭解這些參數與效能之間的關係。下面就是本實驗的詳細步驟(實驗三之一到實驗三之三爲 Postal/SMTP 的相關實驗，實驗三之四及實驗三之五爲 Rabid 相關實驗)：

1. 首先在不修改參數的情形下，對 postal 下基本指令如下

   # postal R615-12.eic.nctu.edu.tw mailsmtp a

   其中 *R615-12.eic.nctu.edu.tw* 爲範例實驗中的 SMTP Server 之位址，而 *mailsmtp* 爲我們的 Mail List，a 無意義，表示我們不使用 conversion-list。觀察 SMTP Mail Server 的 log，以及 postal 的最後結果，計算每分鐘平均能處理的郵件數目。
2. 改變 Process 數目，增加同時間運行的 Process 數目，指令如下：

   # postal -p 10 R615-12.eic.nctu.edu.tw mailsmtp a

   觀察 SMTP Mail Server 的 log，以及 postal 的最後結果，計算每分鐘平均能處理的郵件數目。
3. 回到 1.，改變郵件的大小，分別限定郵件大小在 1K 以下、2K 以下、5K 以下，觀察與 1.的差別，指令如下：

   # postal -m 1 R615-12.eic.nctu.edu.tw mailsmtp a

   # postal -m 2 R615-12.eic.nctu.edu.tw mailsmtp a

   # postal -m 5 R615-12.eic.nctu.edu.tw mailsmtp a
4. 首先在不修改參數的情形下，對 rabid 下基本指令如下

   # rabid R615-12.eic.nctu.edu.tw mailpop a

   其中 *R615-12.eic.nctu.edu.tw* 爲範例實驗中的 POP Server 之位址，而 *mailpop* 爲我們的 Mail List(含 password)，a 無意義，表示我們不使用 conversion-list。

   觀察 POP Mail Server 的 log，以及 rabid 的最後結果，計算每分鐘平均能處理的郵件數目。
5. 改變 Process 數目，增加同時間運行的 Process 數目，指令如下：

   # rabidl -p 10 R615-12.eic.nctu.edu.tw mailpop a

   觀察 POP Mail Server 的 log，以及 rabid 的最後結果，計算每分鐘平均能處理的郵件數目。

Postal 的結果輸出格式範例如下:

time, messages, data(K), errors, connections, SSL connections

15:50,185,1122,0,187,0

說明如下

time: 這整行輸出每分鐘會印出一次，time 紀錄的是本次紀錄的時間，本例中爲 15:50，則下一次的輸出時間爲 15:51，使用者可以藉由比較每分鐘內輸出的資訊來瞭解 Postal 對機器的效能測試結果。

messages: 本分鐘內嘗試送出的訊息。

data(K): 本分鐘內送出的資料量。

errors: 本分鐘內失敗的連線數。

connections: 本分鐘內成功的一般(non-SSL)連線數。

SSL connection: 本分鐘內成功的 SSL 連線數。

VI. 實驗記錄

實驗一：網路環境建構

本實驗建構一個可以供後續實驗使用的基本網路環境，我們將防火牆及路由器的外部介面設爲伺服器(後續實驗中 Spammer 亦設在此網域)所在網域，而內部介面設爲 End-User 端所在網域(後續實驗中我們將郵件伺服器也設在此網域)，記錄下列實驗結果：

	觀察結果
從 End-User 端(Client 端)接收 HTTP Server 的檔案，是否可以成功？	
從 End-User 端往郵件伺服器端寄信，是否可以成功？	

表六之一

實驗二之一：防火牆支援的通訊協定

	FTP	HTTP	SMTP	POP
防火牆支援的通訊協定				

表六之二

實驗二之二：病毒偵測率

偵測率(被擋除病毒數／總病毒數)	

表六之三

實驗二之三：支援的壓縮檔格式

下面提供市面上常見的各種壓縮檔，同學們可以查詢各壓縮檔資料，找出相

對應的編／解碼器，並且測試防火牆是否支援掃描此種格式的病毒壓縮檔。

壓縮檔格式	是否支援？
7zip	
ace	
bh	
bz2	
bza	
cab	
flp	
gz	
jar	
lha	
pak	
pk3	
rar	
rar.exe	
sqx	
tar	
tgz	
yz1	
zip	
zip.exe	

表六之四

實驗二之四：多檔壓縮檔清除(clean)病毒功能的驗證

在病毒壓縮檔掃描的過程中，若壓縮檔中包含健康檔案與病毒檔案，則我們定義 clean 這種清除方式如下：clean 的定義: 接收、(解壓縮)、清除病毒檔、(壓縮)、送出。防火牆是否支援 clean 的功能？

實驗二之五：多檔傳輸時是否會留下健康檔案而檔除病毒檔？

某些廠商對於掃毒的過程較爲嚴苛，若一個 session 中（例如 FTP Session）偵測到一個病毒檔案，便將整個 session 給檔除(block)。此種方法較嚴苛卻較不接近一般使用習慣，且接下來的正常檔案皆無法下載，測試您手上的防火牆，在一次多檔傳輸時(multiple files in a session)，是否會造成 block 的現象？

	FTP	HTTP	SMTP	POP3
是否有 block 現象？				

表六之五

實驗二之六：多層壓縮檔的偵測支援

在網路流通環境下，惡意的使用者往往將病毒檔多次壓縮(Recursively Compressed)以僞裝成一般檔案，驗證你的機器是否支援多層壓縮檔的偵測，如果有，可以偵測到幾層？

在這裡我們必須注意兩點，首先，若是正常的健康檔案，我們必須放行(pass)，若是病毒檔案，則必須檔除，也因此我們必須準備健康的多層壓縮檔與受感染的多層壓縮檔各一，以正確驗證此實驗分項。

	是否支援多層壓縮檔的掃描？	若有，則最多支援的層數(以 100 層爲上限)
受感染的多層壓縮檔		

表六之六

	是否造成誤判的情形？
健康的多層壓縮檔	

表六之七

實驗二之七：單一通訊協定下多埠監測

傳統的防火牆通常對於某些標準的通訊協定僅支援預設 port 的監測，但是各種通訊協定下的 Server 應用程式多可支援更改預設埠的功能，測試您的防火牆，看看機器是否支援單一通訊協定下多埠的偵測。

實驗三之一：黑名單／白名單

這個實驗如圖五之三，爲執行本實驗，我們將三台機器設爲同一網域。首先我們使用 nslookup 指令查詢 Spammer 的網域名稱，將其網域加入黑名單內，從 Spammer 往 End-User 機器寄信，紀錄結果(一)。從 End-User 端自己往自己寄一封信，觀察結果，紀錄結果(二)。

接著我們將 End-User 的完整網域名稱(即機器位址+網域名稱)加入白名單內，自己往自己寄一封信件，觀察結果，紀錄結果(三)，重覆一開始的步驟，從 Spammer 往 End-User 寄信，紀錄結果(四)。

		觀察結果
結果(一)：	僅設定黑名單，是否可以從 End-User 端收到從 Spammer 端寄來的信件？	
結果(二)：	僅設定黑名單，是否可以從 End-User 端收到從自己寄出的信件？	
結果(三)：	設定黑名單與白名單，是否可以從 End-User 端收到從 Spammer 端寄來的信件？	

結果(四)：　設定黑名單與白名單，是否可以從 End-User 端收到從自己寄出的信件？	

表六之八：黑名單與白名單設定結果

實驗三之二：頻率

首先我們已經瞭解垃圾郵件通常是短時間內大量地出現，在 Spammer 位址不在白名單內的前提之下，將 Frequency Check 設爲 100 封／分鐘，記錄下列表格：

	觀察結果
僅從 Spammer 往 End-User 寄出一封信，是否可以收到信件？	
從 Spammer 往 End-User 寄出十封信，時間不限，是否可以收到信件？	
設定 Spammer，大量向 End-User 網域寄出信件(每分鐘必須超過 300 封，若不知如何設定可以使用 Postal 完成此功能)，是否可以收到”任何”信件？	

表六之九

實驗三之三：DNS 反查

首先我們設定 End-User 以及郵件伺服器還有防火牆的 DNS 爲一台合法的 DNS Server(例如交大校內可設 140.113.6.2)，接著將一個不合法的位址分配給 Spammer，此位址必須不能爲 DNS 伺服器所解析，然後從 Spammer 往 End-User 寄信，觀察 End-User 是否能收到信件，紀錄結果(一)，接著將 Spammer 位址移回合法網域內(或者如實驗三之一一開始所設定)，從 Spammer 往 End-User 寄信，觀察 End-User 是否能收到信件，紀錄結果(二)。

	觀察結果
結果(一)：信件來自非法的網域位址，是否可以接收到郵件？	
結果(二)：信件來自合法的網域位址，是否可以接收到郵件？	

表六之十

實驗三之四：Banned Word／過濾垃圾郵件常出現單字及名詞

我們知道大部分的垃圾郵件多是關於色情，藥品以及各項關於優惠／免費的廣告商品，因此我們使用這三類的字眼來當作本實驗的測試範本。將防火牆的 Banned Word 設成下列的單字，寄出給予的範本，觀察結果並紀錄之。並且參考問題與討論(13)，探討本實驗的意義。

Banned Word	Spam 信件範本	觀察結果
性	“…想要看性感小野貓的照片嗎？請上 http:// …”	
性	“…觀察指出，男性的壓力在四十歲前後到達高峰期…”	
藥	“…想要重振雄風嗎？請看看我們藥品強大的效果…”	
藥	“…古人說的好，權力是春藥，很少有人能夠抗拒它的魅力…”	
免費	“…最新型錄！每日前十名登入者免費贈送…”	
免費	“…本實驗探討的是如何使用流程的精簡避免費用的浪費…”	

表六之十一

實驗四之一：Postal 基本運作

Postal 在不給任何參數(除了 SMTP Server Address 跟 Mail-list)的情形下，仍然可以依預設的參數內容運行。本實驗分項在於讓同學瞭解 Postal 的基本運作，下下列指令

postal *smtp-server-address smtp-mail-list a*

觀察前五分鐘 postal 的輸出，記錄下列表格:

總傳輸資料量 (K)	
總成功傳送郵件數／總錯誤(失敗)郵件數 (封)	
平均每分鐘處理資料量 (K／分鐘)	
平均每分鐘處理郵件數 (封／分鐘)	
失敗率 (%)	

表六之十二

實驗四之二：Process 數目對 Postal 運作的影響

爲模擬真實世界的狀態，Postal 亦可以以多緒執行，本實驗中我們增加同時

間運行的 Process 數目，指令如下：

 # postal -p 10 smtp-server-address smtp-mail-list a

觀察前十分鐘 SMTP Mail Server 的 log，以及 postal 的最後結果，計算平均每分鐘能處理的郵件數目並且與實驗四之一的結果比較。需要注意的是，Process 數目必須大於 smtp-mail-list 裡面的帳號名單人數。

總傳輸資料量 (K)	
總成功傳送郵件數／總錯誤(失敗)郵件數 (封)	
平均每分鐘處理資料量 (K／分鐘)	
平均每分鐘處理郵件數 (封／分鐘)	
失敗率 (%)	

表六之十三

實驗四之三：郵件大小對 Postal 運作的影響

這個部份的實驗在於探討郵件的大小隊 Postal 運作的影響，在硬體的測試環境中，例如 Spirent 的 SmartBits/Avalanche，限制信件的大小是一項重要的測試條件，Postal 亦提供這項功能，我們將信件大小分成三個階級，1K 以下、2K 以下、5K 以下(預設值是 10，若爲 0 則代表送出僅有檔頭的信件)，指令分別如下:

 # postal -m 1 smtp-server-address smtp-mail-list a

 # postal -m 2 smtp-server-address smtp-mail-list a

 # postal -m 5 smtp-server-address smtp-mail-list a

分別觀察前五分鐘資料，記錄下表資訊，加以探討原因:

	Under 1K	Under 2K	Under 5K
總傳輸資料量 (K)			
總成功傳送郵件數／總錯誤(失敗)郵件數 (封)			
平均每分鐘處理資料量 (K／分鐘)			
平均每分鐘處理郵件數 (封／分鐘)			

失敗率 (%)			

表六之十四

實驗四之四：Rabid 基本運作

本實驗分項的目的在於讓同學瞭解 rabid 的運作原理，在不下額外控制指令的情形下觀察 rabid 與 POP Server 的運作情形，下以下指令:

rabid *pop-server-address smtp-mail-list a*

觀察 POP Mail Server 的 log，以及 rabid 的最後結果，計算每分鐘平均能處理的郵件數目並且記錄下列表格。

總傳輸資料量 (K)	
總成功連線數／總錯誤(失敗)郵件數 (封)	
平均每分鐘處理資料量 (K／分鐘)	
平均每分鐘處理連線數 (次／分鐘)	
失敗率 (%)	

表六之十五

實驗四之五：Process 數目對於 Rabid 的運作之影響

如同 Postal 之於 SMTP Server，Rabid 亦能以多緒執行來模擬真實世界的環境，我們增加 rabid 同時運行的 Process 數，指令如下:

rabidl *-p 10 pop-server-address smtp-mail-list a*

觀察結果以紀錄表格，並且與實驗四之五比較:

總傳輸資料量 (K)	
總成功連線數／總錯誤(失敗)郵件數 (封)	
平均每分鐘處理資料量 (K／分鐘)	
平均每分鐘處理連線數 (次／分鐘)	
失敗率 (%)	

表六之十六

Ⅶ. 問題與討論

1. 在垃圾郵件的發送手法中，最傳統的方法爲上聊天室或者留言版等易留下個人資訊的地方蒐集帳號，但是這種方法不但費時亦相當不經濟。於是後來許多垃圾郵件發送者便改用字典隨機產生帳號，一次向伺服器送出大量的垃圾信件，並根據伺服器回傳不存在帳號的資料，砍除字典隨機產生的帳號群。這種方法不但一次就可以得大量有效的帳號，而且對垃圾郵件發送者來說亦較省時省力。這種方式不但造成垃圾郵件的廣泛猖獗，亦容易造成系統服務的癱瘓(Denial of Service)，是否有簡單有效的防治方法？
2. 傳統已架設 Anti-Spam 系統的廠商，有時仍然遭受垃圾郵件之侵擾，原因之一在於 Anti-Spam 系統架設的不周延，以至於無法強制所有進入公司的郵件均經過 Anti-Spam 系統，試想一種可以防治繞道發送的簡單架構。
3. 在表三之二中，我們提到一種可以依據垃圾郵件常出現字眼來過濾垃圾郵件的方式，但是新型態的垃圾郵件不但會插入許多不相關的網站連結，甚至會將字句的排列做自動拆換，以規避自動學習或防堵工具，是否有任何方法可以排除這種新型態的垃圾郵件？
4. 在實驗四之二與四之五的結果中，您觀察同時間執行的 Process 數目與 Server 效能的關係爲何？對照真實世界的運行，一個良好的郵件系統，該有怎麼樣的機制來處理系統過載的情形？
5. 在實驗四之三中，我們觀察到郵件大小與伺服器效能之間的關係，就你的觀察，郵件大小如何影響伺服器效能？原因又爲何？
6. 在您實驗四的結果中，是否有錯誤的情形產生？若有，您覺得造成錯誤的原因爲何？若沒有任何錯誤的情形產生，同學可以討論出一種或者一種以上在真實世界中會造成錯誤的情形。
7. 在實驗二之三中，我們觀察到不同的機器與環境會對不同的壓縮格式有不同的支援度，這裡所謂的支援度，一方面指的是”支援的格式總數”，另一方面指的是”對於流行格式的支援性”，例如 ZIP、RAR 等常見的格式，從實驗的結果轉換到真實世界，您覺得哪一種是廠商比較該著力的部份？
8. 在實驗二之六中，我們看到實驗環境對多層壓縮檔可能有誤擋的情形，也就是機器會將健康的多層壓縮檔當成病毒直接擋除(blocked)，這種情形一方面是因爲廠商策略：對於多層壓縮檔直接擋除以免降低整體系統效能，另一方面也有可能廠商對於無法處理辨識的資料直接當成病毒，觀察您的結果，是否能正確的分辨壓縮的健康與病毒檔案，觀察能正常判別的機器以及其他策略的機器，他們在處理多層壓縮檔上的速度是否有明顯差異？
9. 在 HTTP 的通訊協定中，我們直覺地會測試下載部分的防毒功能，然而在實際應用中，HTTP 協定亦支援上傳的功能，這個部份是許多防火牆未著墨的死角，請列舉數種使用到 HTTP 協定中上傳功能的實例，並且探討防火牆爲

何需要考慮這部份流量的必要性。

10. DNS 反查爲現在各家 Anti-Spam 廠商最主要的防止垃圾郵件機制之一，這個機制主要是針對傳送至企業的電子郵件之 IP 位址，以反查的方式來確認出傳送郵件的主機名稱，請說明當一台具 DNS 反查功能的機器遭遇到許多不同網域來源的信件時，可能遇到的問題，並且詳述這種缺點的原因。
11. 在這次防堵垃圾郵件的實驗中，我們測試了黑名單與白名單的機制，請說明爲什麼這兩種機制需要相輔相成而不宜單獨使用的理由。
12. 在 SMTP 通訊協定中，由於早期的設計爲信任使用者的機制，故 SMTP 伺服器在未特別設定的情形下，可以視爲一個無限制 Relay 的 Server，請上網蒐集資料，探討新一代的郵件伺服器軟體如何克服這一項先天上的缺陷？
13. 從實驗三之四我們可以得知，傳統 banned word 並不十分的精確，往往造成大量的誤判，請上網蒐集資料，探討新型的 banned word 如何使用智慧型的方式判別信件。亦可以參考參考文獻[6]。
14. 請探討各項 Anti-Spam Pattern 的優先次序，例如決定黑名單白名單與 Banned Word 的優先判定次序。範例如下，如果一封信在白名單內，就不再檢查 Banned Word，指出本次實驗中哪項 Pattern 該給予最高的優先次序？

Ⅷ. 參考文獻

[1] 資安人, “圍堵垃圾郵件面面觀”, No. 17, Mar., 2005

[2] 網路通訊, “亞洲垃圾郵件面面觀”, No. 163, Feb., 2005

[3] 網路通訊, “看穿病毒，一擊必殺”, No. 167, Jun., 2005

[4] 資安人, “防毒技術支援服務深入測試”, No. 13, Oct., 2004

[5] Postal – SMTP and POP benchmark program, http://www.coker.com.au/postal/

[6] 科學人, “終結垃圾信”, May, 2005, http://www.sciam.com.tw/read/readshow.asp?FDocNo=672&CL=19

[7] 網路通訊, “電子郵件的愛恨情仇－POP3”, No. 162, Jan, 2005

[8] Spirent: Smartbits/Avalanche http://www.spirentcom.com/news/press.cfm?id=1055

[9] Fortinet Anti-Spam Filter Order http://kc.forticare.com/default.asp?SID=&Lang=1&id=539

[10] 如何確保 e-mail 能讓對方收到？(1) DNS 反查篇 http://www.url.com.tw/include/index/topic/home-info/email_faq/dns1.shtm