스팸메일 릴레이 방지

2002. 5. 3

한국정보보호진흥원
기반보호사업단/해킹바이러스상담지원센터
김상철선임연구원(kims@certcc.or.kr)
이완희연구원 lwh@certcc.or.kr

1. 개요

최근에 이메일 추출기의 판매 및 이메일 주소의 매매 행위로 인해 스팸 메일이 극성을 부리면서 스팸 메일을 지우는 데에 많은 시간을 소비하고 있다. 그리고 최근에 우리나라가 세계적인 스팸메일 발생지 및 릴레이서버로 보도되어 일부 IP 대역이 블록 되는 일까지 일어나

릴레이 관련 설정을 확인할 필요가 있다.

2. 각 메일서버별 스팸메일 릴레이 방지 설정

1) Sendmail

본 문서에서는 국내에서 가장 많이 사용되고 있는 메일서버의 MTA인 Sendmail에 대한 스팸릴레이 대응방법에 대하여 기술하여 국내에서 사용되는 메일서버가 스팸릴레이 서버로 악용되는 것을 예방하고자 한다.

※ Sendmail 설치방법

Sendmail 가져오기 및 준비하기

o 가장 최근의 Sendmail버전은 http://www.sendmail.org/의 웹사이트에서 무료로

제공
- 8.12.X버전이 최근버전임

o 다운로드된 Sendmail프로그램을 설치하기 위해서는 C/C++ 컴파일러가 반드시 설치되어 있어야 함

o Sendmail은 무료로 배포되고 있는 GNU/gcc로 컴파일 가능.
- 리눅스는 GNU/gcc가 자동 디폴트로 설치되어 있으며, UNIX(Solaris, AIX 등)는 벤더사이트나, GNU사이트에서 다운로드 가능

※ Sendmail 설치하기

o Sendmail의 스팸 릴레이 차단기능은 8.9.0 이후의 버전부터 완전하게 지원하기 때문에, 기존에 설치된 Sendmail의 버전을 확인 필요

- 버전을 확인하는 방법은 Sendmail이 구동될 때 이용되는 환경변수파일인 sendmail.cf파일의 "# Configuration version number" DZ8.9.1라인의 정보를 통하여 확인가능
- 대부분의 sendmail.cf파일은 /etc디렉토리나 /etc/mail디렉토리에 설치되어 있음

o Sendmail 8.11.6의 설치(SunOS 5.7, solaris 7)

① 다운로드 받은 sendmail.8.11.6.tar.gz파일을 설치하고자 하는 Sendmail서버로 Ftp 프로그램을 사용하여 메일서버로 전송
- 설치 디렉토리는 상관없음.

② gzip과 tar명령어를 사용하여 압축해제.

```
[penguin:root]:/user1/ksch/gzip -d sendmail.8.11.6.tar.gz

[penguin:root]:/user1/ksch/tax cvf sendmail.8.11.6.tar
```

③ sendmail의 설치디렉토리에서 "sh Build" 명령의 실행을 통하여 sendmail 설치환경 구성

```
[penguin:root]:/user1/ksch/sendmail-8.11.6> ls
./      INSTALL     PGPKEYS     contrib/    libmilter/  mailstats/  sendmail/
../     KNOWNBUGS   README      devtools/   libsmdb/    makemap/    smrsh/
Build   LICENSE     RELEASE_NOTES  doc/     libsmutil/  praliases/  test/
FAQ     Makefile    cf/         include/    mail.local/ rmail/      vacation/

[penguin:root]:/user1/ksch/sendmail-8.11.6> sh Build
```

※ groff가 설치되어 있지 않으면, 컴파일 과정에서 에러가 발생할 수 있으며, 메뉴얼 페이지를 사용하지 않으면 무시해도 괜찮음.

④ sendmail의 설치디렉토리의 하위 디렉토리인 cf/cf디렉토리에서 설치하고자 하는 시스템과 일치하는 .mc파일을 config.mc로 복사(SunOS5.7인 경우)

- sendmail이 설치되는 각각의 OS에 맞는 .mc파일이 존재함.
- SUN Solaris 2.X버전은 generic-solaris2.mc 파일을 사용

```
[penguin:root]:/user1/ksch/sendmail-8.11.6/cf/cf> ls
./                  cs-solaris2.mc      generic-hpux9.mc    generic-sunos4.1.cf
../                 cs-sunos4.1.mc      generic-linux.cf    generic-sunos4.1.mc
Build*              s2k-osf1.mc         python.cs.mc        cs-ultrix4.mc
generic-linux.mc    generic-ultrix4.cf  s2k-ultrix4.mc      Makefile
cyrusproto.mc       generic-ultrix4.mc  tcpproto.mc         cs-hpux9.mc
chez.cs.mc          generic-bsd4.4.cf   huginn.cs.mc        ucbarpa.mc
clientproto.mc      generic-bsd4.4.mc   generic-osf1.cf     knecht.mc
cs-hpux10.mc        generic-hpux10.cf   generic-osf1.mc     mail.cs.mc
generic-hpux10.mc   generic-solaris2.cf mail.eecs.mc        vangogh.cs.mc
cs-osf1.mc          generic-hpux9.cf    ucbvax.mc           mailspool.cs.mc
generic-nextstep3.3.mc generic-nextstep3.3.cf generic-solaris2.mc uucpproto.mc

[penguin:root]:/user1/ksch/sendmail-8.11.6/cf/cf> cp generic-solaris2.mc config.mc
```

⑤ 생성된 config.mc파일을 사용하여 config.cf파일 생성

```
[penguin:root]:/user1/ksch/sendmail-8.11.6/cf/cf> sh Build config.cf

Using M4=/usr/ccs/bin/m4
rm -f config.cf
/usr/ccs/bin/m4 ../m4/cf.m4 config.mc > config.cf || ( rm -f config.cf && exit 1 )
chmod 444 config.cf
```

⑥ 구버전의 /etc/mail/sendmail.cf 파일 백업
- 일부 시스템은 /etc/sendmail.cf파일을 사용하므로 주의요망.
- cp, mv, tar등의 명령어를 사용

```
[penguin:root]:/etc/mail/cp sendmail.cf /백업디렉토리/sendmail.cf

[penguin:root]:/etc/mail/mv sendmail.cf /백업디렉토리/sendmail.cf
```

⑦ 설치된 sendmail/ 디렉토리에서 "sh Build install"명령 실행한 후에 config.cf파일을 /etc/mail/sendmail.cf파일로 Copy명령어를 사용하여 설치

```
[penguin:root]:/user1/ksch/sendmail-8.11.6> sh Build install
Making all in:
/user1/ksch/sendmail-8.11.6/libsmutil
Configuration: pfx=, os=SunOS, rel=5.7, rbase=5, rroot=5.7, arch=sun4, sfx=,
variant=optimized
......

[penguin:root]:/user1/ksch/sendmail-8.11.6> cp ./cf/cf/config.cf /etc/mail/sendmail.cf
```

⑧ sendmail과 관련된 도구들(makemap, mailstats, 기타등등)의 설치
- 각각의 도구들의 디렉토리에서 README파일을 숙지한 후에 "sh Build install"실행

```
[penguin:root]:/user1/ksch/sendmail-8.11.6/makemap> ls
./  ../  Build*  Makefile  Makefile.m4  makemap.0  makemap.8  makemap.c

[penguin:root]:/user1/ksch/sendmail-8.11.6/makemap> sh Build install
```

⑨ 새로운 버전의 makemap도구를 사용하여 Database Maps을 생성
※ 2.3절의 Sendmail Spam Relay기능 설정하기 참조

⑩ /etc/mail/local-host-names파일을 생성하여 메일서버의 호스트명 입력

```
[penguin:root]:/etc/mai▷ cat  local-host-names
penguin                         <== 메일서버의 호스트 이름
penguin.certcc.or.kr            <== 메일서버의 도메인 이름
```

⑪ Sendmail의 설치 및 컴파일등에 대한 상세한 설치방법 및 자료에 대해서는 다음 페이지를 참조하기 바란다.

- http://www.sendmail.org/compiling.html
- http://www.plus.or.kr/document/etc/sendmail.html

※ Sendmail Spam Relay기능 설정하기

o Sendmail8.9.0부터는 디폴트로 메일 릴레이 기능을 제한하도록 되어 있으며 이러한 기능들을 제어하기 위한 많은 환경변수들을 제공

o 환경변수들은 sendmail.cf파일에 저장되어 지는데, 많은 관리자들이 Sendmail 프로그램을 설치하는데 있어 가장 애로를 겪는 부분임

o Sendmail이 anti-spam 기능이 있다고 해도, 이 파일을 적절히 만들어 적용하지 못하면 무용지물이 되기 때문에 관리자들은 이 파일의 적용방법을 반드시 숙지하여 운영하여야 함

o Sendmail 8.9로 버전이 높아지면서 새롭게 추가된 기능이 바로 이 anti-spam과 관련된 기능이며 Access DB라는 새로운 데이터베이스를 도입해서 이것의 설정에 따라 특정 메일들을 받지 않도록 할 수가 있음

o 그 내부 형식은 다음의 표와 같다.

spam@hacker.com	REJECT
spammail.com	REJECT
useful.org	OK
211.252.150	RELAY
211.252.151	RELAY

- spam@hacker.com, spammail.com 및 211.252.150과 같은 첫번째 필드는 e-mail 주소, 도메인 네임, 네트웍 넘버 등이 올 수 있으며,

- 두번째 필드는 해당 주소로부터 오는 메일을 어떻게 처리할 것인가를 결정하는 데에 사용

- spam@hacker.com의 메일사용자 및 spammail.com 도메인으로 부터 오는 모든 메일은 거절

- useful.org 도메인으로부터 오는 모든 메일은 받아들인다는 설정

- 마지막의 것은 C-Class의 네트워크가 211.252.150, 211.252.151의 IP를 사용하는 모든 IP주소에 대하여 릴레이를 허가

o 위와 같은 형식의 access DB는 /etc/mail/access란 이름으로 파일 시스템에 저장

o access의 파일구조는 텍스트 파일이며, Sendmail이 참조(Lookup)할 수가 없음

o makemap이란 프로그램을 사용하여 Sendmail이 인식할 수 있는 DB 형태로 만들어 주어야 함

- 다음의 명령어를 실행하여 가능 "/etc/mail/makemap dbm /etc/mail/access < /etc/mail/access"

- 디렉토리를 /etc/mail으로 옮긴다음 위와 같은 명령을 쳐주면, access.dir과 access.pag라는 이름으로 DB가 생성됨

- /etc/mail/access 파일을 수정할 때마다 makemap을 사용해 새롭게 DB를 만들어 주어야 함

o 버클리 DB를 이용한다면 약간 형식이 틀려지는데, 그럴 때는 다음과 같이 hash 옵션을 사용하여야 함.

/etc/mail/makemap hash /etc/mail/access < /etc/mail/access

o 다음의 표는 이러한 access파일을 통하여 sendmail이 참조할 수 있는 Access DB 파일을 생성하는 방법 및 과정을 보여줌

```
[penguin:root]:/etc/mail> ls -al access*
-rw-r--r--   1 root     other          71  5월  3일  17:25 access

[penguin:root]:/etc/mail> cat access
spam@hacker.com REJECT
spammail.com    REJECT
useful.org      OK
172.16          RELAY

[penguin:root]:/etc/mail> makemap dbm /etc/mail/access < /etc/mail/access

[penguin:root]:/etc/mail> ls -al access*
-rw-r--r--   1 root     other          71  5월  3일  17:25 access
-rw-r--r--   1 root     other           0  5월  3일  17:27 access.dir
-rw-r--r--   1 root     other        1024  5월  3일  17:27 access.pag

[penguin:root]:/etc/mail> cat access.pag
家詳鳩믄RELAY172.16OKuseful.orgREJECTspammail.comREJECTspam@hacker.com
```

o 이러한 환경파라미터들의 상세한 내용에 대한 설정을 올바르게 사용하기 위해서는 cf/README 파일의 Anti-Spam 환경제어 부분을 참조하기 바란다.
  - http://www.sendmail.org/tips/relaying.html
  - http://www.sendmail.org/m4/anti-spam.html

o 대부분의 이러한 Anti-Spam Relay 솔루션들은 메일관리자가 허용되는 Relay 도메인들의 리스트들을 설정하는 것을 필요로 한다. 이 리스트에는 모든 허가 인증된 도메인들를 포함하고 있는지 반드시 확인하여야 하며 주의하여야 할점은 반드시 MX (Mail Exchanger)뿐만 아니라 당신의 도메인에서 사용하고 있는 가상의 도메인들이 포함되도록 설정하여야 한다. 그렇지 않으면 당신이 보낸 메일이 거절될 수도 있을 것이다.

o 메일 서버가 FEATURE(relay_entire_domain)을 사용해서 8.9.x버전 이상의 sendmail을 구성하였다면, 이는 도메인 내에 있는 모든 호스트로부터의 릴레이를 허용한다는 것을 의미한다. 만약 "relay_entire_domain"이 호스트 이름("host." : host.domain.com)을 사용한다면 디폴트로 sendmail은 당신의 시스템에 있는 모든 IP 주소를 체크해서 "reverse lookups"를 수행하여 메일서버의 시스템부하를 가중시키게 될 것이다.

o Spam Relay의 가장 좋은 해결방법은 .cf파일을 포함하여 relay_entire_domain을 사용하는 대신에 IP주소를 사용하여 Relay호스트를 설정하는 것이 설정상의 오류를 해결할 수 있는 좋은 방법이 될 수 있다..

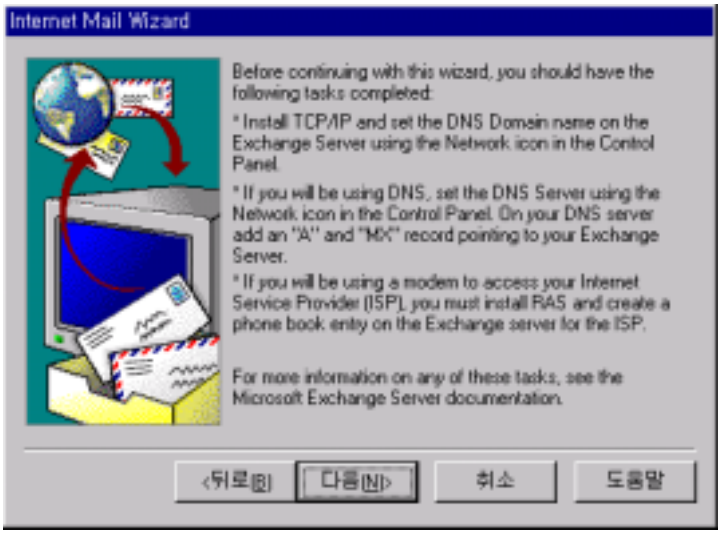
2) Microsoft Exchange Server

본 문서에서는 마이크로소프트사에서 제공하고 있는 메일서버인 Exchange Server에 대한 스팸릴레이 대응방법에 대하여 기술하여 국내에서 사용되는 메일서버가 스팸릴레이 서버로 악용되는 것을 예방하고자 한다.

※ IMS 설치방법

o Exchange Server를 설치후 맨먼저 Microsoft Exchange Administor를 실행시켜 "File" 메뉴에서 "New Other"를 선택한 다음 'Internet Mail service...' 를 선택한다.

o 인터넷 메일 서비스를 설치하기전에 DNS(Domain Name Service)에 반드시 메일서버 관련 사항을 설정하라고 명시하고 있다.



o IMS가 설치될 서버를 지정한다. (대부분 현재 자신의 메일서버이다.)

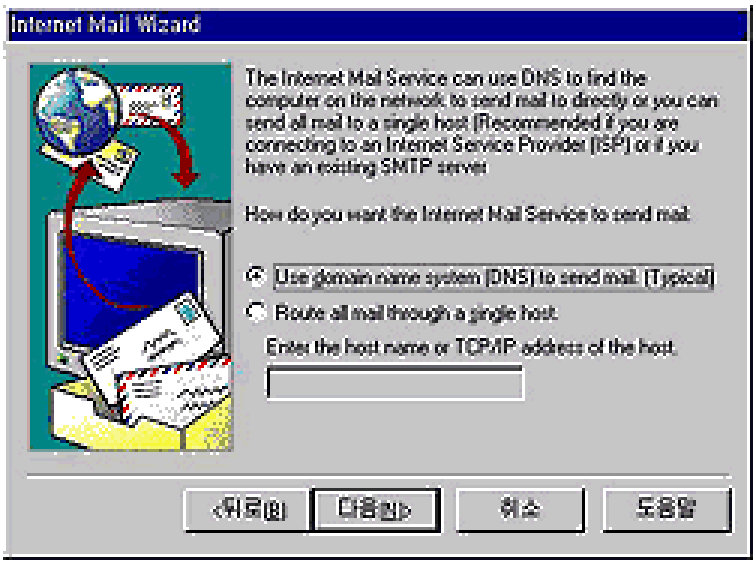
o IMS 가 메일 메시지를 전송할 때 DNS 서비스를 이용해서 수신할 서버와 직접 연결할 것인지 아니면 메일을 relay 서버로만 보내고 최종 수신지 서버와는 relay 서버가 통신하도록 할 것인지를 지정하는 화면이다.

- Use Domain name system... 을 선택하는 것이 보통의 경우이다.
- Route all mail through... 가 relay 서버를 이용하는 경우이다.

o 다음 설정은 송신주소를 제한하는 설정으로 첫 번째 기본 옵션을 선택한다.

o 다음은 SMTP 메일 어드레스의 @ 뒷부분을 지정하는 화면이다.
기본적으로는 @site-name.serve-name 으로 지정된다. 하지만, SMTP 메일은 @ 뒷부분의 DNS 명을 가지고 서버와 연결을 시도하므로, 아무렇게나 지정하면 안 된다.
@ 뒷부분은 DNS 에 명기된 이름이어야만 SMTP가 이 서버와 접속 할 수 있다.
대부분은 서버자신의 DNS 명이 될 것이다. (예 @mail.certcc.or.kr)

o 다음은 인터넷 메일의 관리자용 메일박스를 지정하는 설정이다



o 마지막으로 이 서비스를 기동시킬 서비스 계정을 지정하는 화면이다.

o 설치가 완료된 후 일단 서비스가 정상적으로 실행되었는지 제어판에서 '서비스'를 선택하여 'Microsoft Exchange Internet Mail Service' 가 시작되었는지 확인한다.

※ 릴레이 설정을 통한 릴레이 방지

- **Exchange Server 5.5 SP1 이후 버전으로 업그레이드할 수 없는 경우**
  - 레지스트리 키를 추가하여 릴레이(Relay) 제한을 구성할 수 있다.

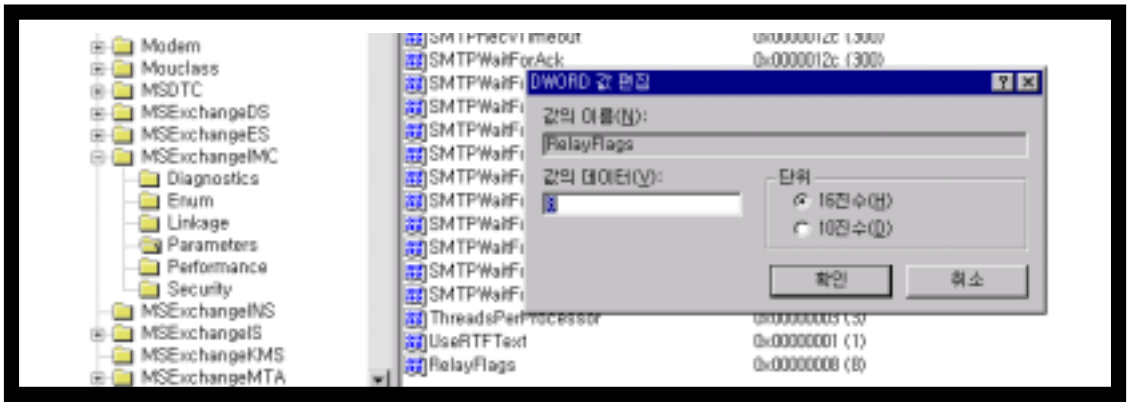
다음 레지스트리 키 값을 사용하여

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Service\MSExchangeIMC\Parameters

아래 레지스트리 값을 추가하여 릴레이(Relay) 제한을 구성하기 바란다.

o 추가할 레지스트리 값
RelayFlags, RelayDenyList, RelayAllowList, RelayLocalIPList

① RelayFlags, REG_DWORD (이름, 데이터 유형)
- 어떤 릴레이(Relay) 제어 규칙을 사용하는지 정의한다.



- **RelayFlags 세부 설정**

o RelayFlags가 비트 1로 설정(십진수 1)되고 클라이언트의 IP 주소가 RelayDenyList의 패턴과 일치하는 경우 클라이언트는 메일을 릴레이(Relay)할 수 없습니다.

o RelayFlags가 비트 2로 설정(십진수 2)되고 클라이언트의 IP 주소가 RelayAllowList의 패턴과 일치하는 경우 클라이언트는 메일을 릴레이(Relay)할 수 있습니다.

o RelayFlags가 비트 3으로 설정(십진수 4)되고 클라이언트의 IP 주소가 RelayLocalList의 패턴과 일치하는 경우 클라이언트는 메일을 릴레이(Relay)할 수 있습니다.

o RelayFlags가 비트 4로 설정(십진수 8)되고 클라이언트가 인증을 얻는 경우 클라이언트는 메일을 릴레이(Relay)할 수 있습니다.

② RelayDenyList, REG_MULTI_SZ
- 서버를 통해 메시지를 릴레이(Relay)할 수 없는 호스트를 지정한다.

RelayDenyList, RelayAllowList 및 RelayLocalIPList는 행 당 네트 주소 및 옵션 마스크 하나로 이루어져 있다. 각 행(Line)은 두 부분, 즉 세미콜론(;)으로 분리된 네트 주소 및 마스크로 이루어진다. 예를 들면, 다음과 같다. => 192.168.0.0;255.255.0.0
Net[:mask] 마스크가 생략되면 기본값 255.255.255.255가 사용된다.

* 주의
데이터 유형중 하나인 REG_MULTI_SZ는 regedit32를 이용하여 값을 추가하여야 한다. 일반 regedit로는 추가가 불가능하다. 그리고 Rededit32에서 제공하는 복수 문자열 편집기를 이용하여 작업을 하여야 한다.

③ RelayAllowList, REG_MULTI_SZ
- 서버를 통해 메시지를 릴레이(Relay)할 수 있는 호스트를 지정한다.

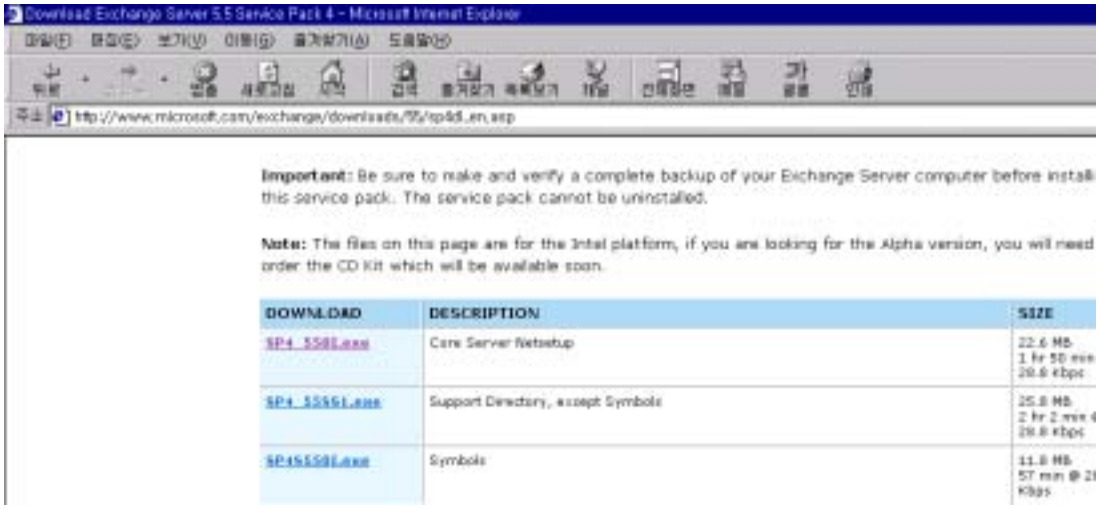
④ RelayLocalIPList, REG_MULTI_SZ
- SMTP 클라이언트가 연결할 수 있고 메일을 릴레이(Relay)할 수 있는 서버의 로컬 IP 주소를 지정한다. 이것은 내부 및 외부 인터페이스가 있는 다중 홈 서버(Multi-homed Server)에 유용하다. IP 전달을 설정하면 이 기능을 사용할 수 없다.

자세한 사항은 아래의 문서를 참조하기 바란다.

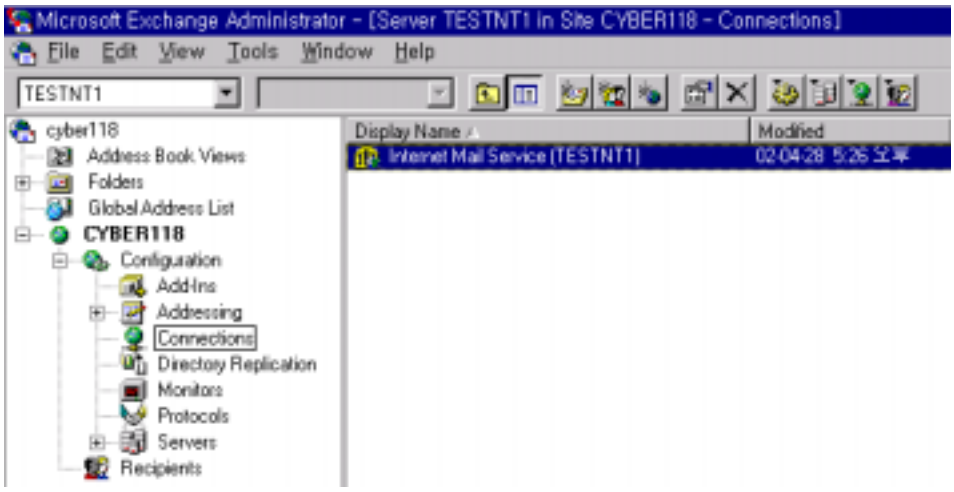
http://support.microsoft.com/default.aspx?scid=%2Fisapi%2Fgomscom%2Easp%3Ftarget%3D%2Fkorea%2Fsupport%2Fxmlkb%2Fkr193922%2Easp&LN=KO

• Exchange Server 5.5 서비스 팩 1이상의 서비스 팩을 설치한 경우

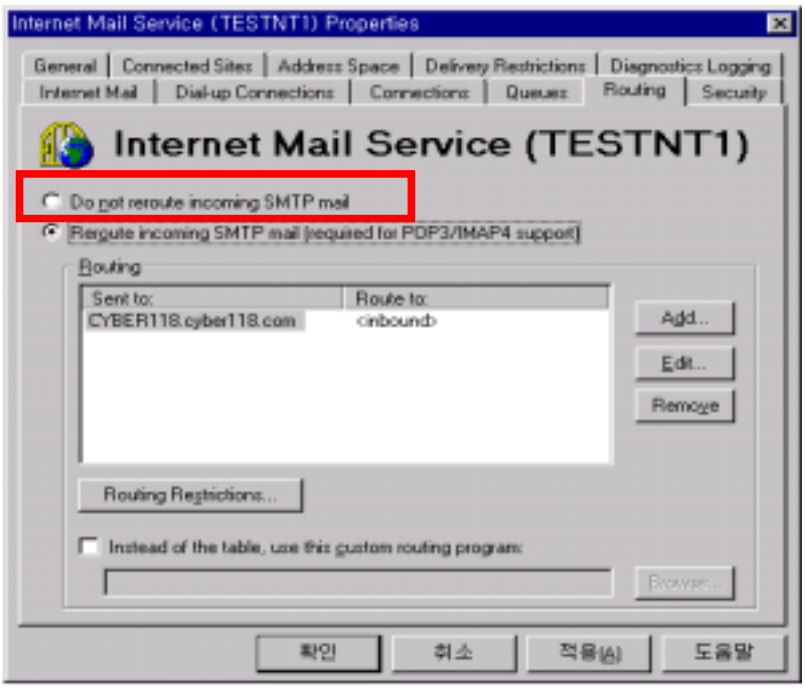
o Exchange Server 5.5의 서비스 팩 1이나 이후 버전의 서비스 팩을 설치한다.
아래의 사이트로 이동하여 최신 서비스팩을 다운 받는다.



o Exchange Server Administrator(관리자) 프로그램에서 Connections에서 Internet Mail Servece를 더블클릭한다.

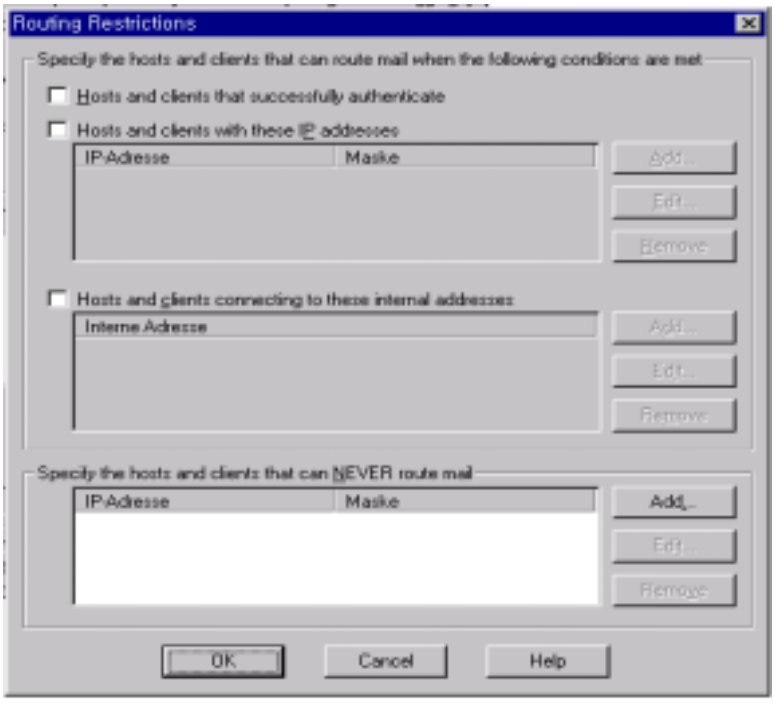


o Internet Mail Servece Properties에서 Routing탭을 선택한다.



o 스팸 릴레이를 허용하지 않으려면 "Do not reroute incoming SMTP mail"를 체크한다.

o 릴레이를 허용하고 제한하기 위해서는 Reroute incoming SMTP mail을 선택 한 다음 Routing Restrictions을 선택한다.



o Specify the hosts and clients that can route mail when the following conditions are met 대화 상자에서 호스팅 옵션을 선택한 다음 Add를 눌러서 제한된 IP 주소를 지

정한다.

o 릴레이를 허용하는 IP를 Hosts and clients with these IP_addresses항목에 입력한다.

o 릴레이를 허용하지 않으려면 Specify the hosts and Clients that can NEVER route mail을 선택한다.

o 서비스를 중지후 재시작한다.

3) EMWAC IMS

최근에 스팸 릴레이 관련된 사고가 늘어나고 있는데 이중 EMWAC 메일 서버를 이용한 스팸릴레이 사고가 다수 접수되고 있다. 이 프로그램은 용량이 적고, 설정이 간단하며, freeware 이기 때문에 많은 사용자들이 사용을 하고 있지만 개발 당시 스팸메일 사고를 고려하지 않고 개발되어 스팸메일(릴레이)을 막기 위해서는 프로그램을 추가 설치해야 한다.

스팸 릴레이를 막기 위해서는 SCSMFILTER Plus 프로그램을 먼저 인스톨하여 필터링하고 플러그 인 프로그램인 Antirelay 프로그램을 인스톨하여서 특정 IP와 도메인의 접근을 차단하여 스팸의 릴레이를 막을 수 있다. 필터링을 설정하기위한 Configuration Manager를실행하여 세부 DAT 파일을 설정해 주면된다.

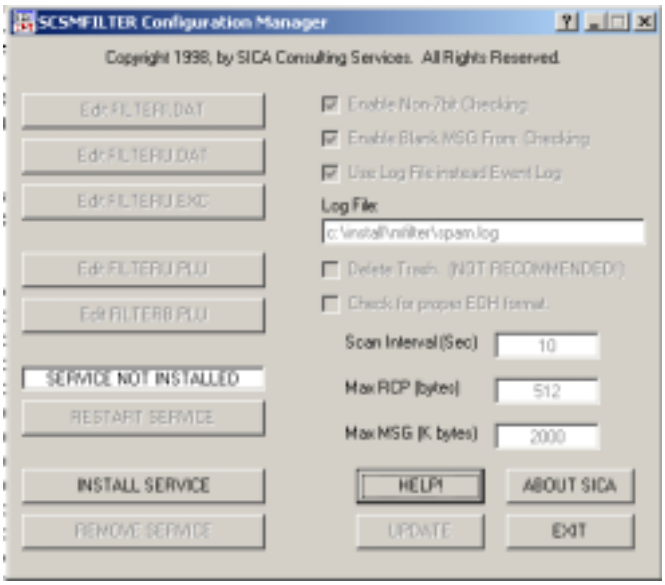
* SCSMFILTER Plus 설치방법

o 아래의 사이트로 가서 SCSMFILTER를 먼저 다운 받는다.
http://www.sica.com/freestul/scsmfilt.htm

o 다운받은 파일의 압축을 풀고 setup 파일을 실행시킨다.

o 임시 폴더에 프로그램을 설치 후 Config.exe를 실행시킨다.

o Configuration Manager 화면에서INSTALL SERVICE를 누릅다.



o EMWAC IMS를 선택하고, Install SCSMFILTER를 누른 뒤 확인하면 된다.

o 설치 완료후 현재 실행되고 있는 SMTP Receiver 서비스를 멈춘후 다시 시작한다.

o 필터링을 적용하는 SCSMFILTERPlusE 서비스를 시작하고, 시스템 -서비스 메뉴에서 SCSMFILTERPlusE 서비스를 시작옵션에서 재 부팅시 에도 자동적으로 실행되도록 자동으로 변경한다.

- 필터링 설정

o Configuration Manager를 실행 한다.

o FILTERI.DAT
파일의 문자열들과 수신 메일 header 부분을 비교하여 일치하는 부분이 있으면 필터링 적용하여 TRASH 폴더로 버린다.

o FILTERU.DAT
수신된 메일헤더의 "From:" 다음에 오는 문자가 일치하면 TRASH 폴더로 보낸다.

o Enable Non-7bit Checking 란을 체크하지 않으면, 8 bits characters 를 필터링하지 않는다. (한글이 8bit를 사용하므로 체크 안함)

o Max RCP (bytes)
RCP 파일은 메일의 송수신자를 나타내는 파일로써 SPAM 을 보내는 사용자가 수신자를 CC로 묶어서 보낼경우 RCP 파일의 크기가 커지므로 용량제한을 하여 SPAM을 방지하는 방법이다.

* Anti_relay 설치

o antirelay.zip 파일을 다운로드 받은 다음 특정폴더에 압축을 푼다.

o SCSMFILTER Plus Configuration Manager를 실행후 Edit FILTERU.PLU를 클릭한다.

o 아래와 같은 내용을 추가한후 add와 RETURN를 클릭한다.
C:\설치된폴더\antirelay.exe 0 0 C:\설치된폴더\ARgoodIP.dat C:\설치된폴더\ARdomain.dat

- 메일 접근제어

o ARgoodIP.dat
들어오는 메일의 헤더에서 source IP를 확인하여 이미 정의되어 있는 IP이면 메일 송신을 허락한다.

o ARdomain.dat
들어오는 메일의 주소에서 수신 가능한 도메인을 정의한다.
예) xxx.co.kr또는 xxx.com

- 메일 릴레이설정

o Antirelay.exe와 Antirelay.ini를 Mfilter가 설치된 폴더에 복사한다.

o SCSMFILTER Plus Configuration Manager를 실행후 Edit FILTERB.PLU를 클릭한다.

o 아래와 같은 내용을 추가한후 add와 RETURN를 클릭한다.
c\설치한폴더\antirelay.exe c\설치한폴더\antirelay.ini

o antirelay.ini를 수정합니다.

localnets : 이 부분은 relay를 허용하는 IP를 설정한다.
예) net1=172.16.5.0/24 (원하는 IP나 블록)

아래 링크로 가면 플러그인 다운로드 방법과 설정방법을 자세히 설명해 놓았으므로 참조하시기 바랍니다.

http://www.ntfaq.co.kr/emwac/default.asp

4) Qmail

Qmail도 릴레이는 기본적으로 안되게 되어있다. local과 virtualdomains에 있는 도메인 네임들에 있는 완전 도메인네임들을 /var/qmail/control/rcpthosts파일에 적기 때문이다.
릴레이가 필요시에는 릴레이 관련 설정을 확인한 후 테스트를 한후 릴레이를 허용하여야 한다. Qmail에서 릴레이를 두 개의 설정파일로 컨트롤한다. 첫 번째 파일인 /etc/tcp.smtp에서 릴레이와 접근을 막는 설정을 할수 있고 두 번째 파일인 /var/qmail/control/rcpthosts 파일에서는 메일 릴레이를 열어줄 서버를 결정해 준다. 여기서 중요한 것은 rcpthosts파일은 tcp.smtp 설정의 RELAYCLIENT="" 이 옵션이 없을 때에만 동작하며 우선순위를 가진다. 그러므로 rcpthosts 파일에 릴레이가 필요한 IP를 기록하고 모두를 allow하면 먼저 rcpthosts를 확인한후 릴레이를 허용할 IP를 확인한 다음 만약 해당 IP가 없다면 릴레이를 막을 것이다.

아래의 tcp.smtp 설정은 172.16.5.xxx 및 로컬은 모두 허용하고 rcpthosts에 있는 IP를 제외한 모든 IP는 막는다는 뜻이다.

```
172.16.5.:allow,RELAYCLIENT=""
127.0.0.1:allow,RELAYCLIENT=""
:allow
```

tcp.smtp 를 수정한 후에는 tcpserver가 사용할 수 있는 cdb 형식으로 바뀌주기 위해 아래와 같이 db 파일로 바꾸어 주어야 하며 sendmail과 같이 qmail을 재시작 할 필요는 없다.

```
# tcprules /etc/tcp.smtp.cdb /etc/tcp.smtp.tmp < /etc/tcp.smtp
```

특정 IP 대역의 메일 관련 접속을 완전히 막을려면 해당IP:deny 설정을 하여 smtp로의 접속을 완전히 막을수 있다.

qmail 메일도 Sendmail과 같이 유동 IP 사용자들에게 릴레이를 열어 주어야 하는 메일 서버의 경우에는 qmail 소스를 패치하면 qmail-smtpd가 암호 인증 후에 릴레이를 열어주는 방법이 있다. 자세한 것은 아래의 문서를 참조하기 바란다.

http://kldp.org/~eunjea/qmail_relay.php#tcpserver

5) 기타 메일 서버

가) Windows 2000 서버의 기본 SMTP 서버

Windows 2000 서버 설치시 SMTP 서비스는 디폴트로 설치되고 Windows 2000 Professional 설치의 경우에는 선택적으로 설치 가능하다. 최근에 이와 관련된 취약

점으로 인해 허가되지 않은 사용자가 SMTP 서비스에 대해 릴레이 서비스를 이용할 수 있으므로 아래의 사이트에서 패치를 해야한다.
(주의 : 이 취약점은 Windows 2000 메일 서비스를 실행하는 서버에만 영향을 주며 도메인의 멤버 형태보다는 단독형 기기로 구성된 경우에만 영향을 받습니다.)

http://www.microsoft.com/korea/technet/security/bulletin/ms01-037.asp

나) Domino SMTP
Lotus Notes의 Domino 서버에 관한 글은 아래의 링크를 참조하여 릴레이 관련 설정을 하시기 바랍니다.

http://www.notespia.net/

6) 스팸 릴레이 블랙리스트 사이트

http://www.mail-abuse.org는 스팸 블랙리스트를 관리하는 대표적인 사이트로 이 사이트에 스팸리스트로 등록이 되면 특정 도메인으로 메일을 보내는 것이 차단되므로 확인을 해 보시기 바랍니다. 만약 여기 리스트에 등록이 되었다면, 자신의 메일서버의 릴레이를 막으신 후 삭제를 요청하시면 됩니다. 반드시 Relay 거부 설정을 한 후 신청을 해야 처리가 되므로 아래의 문서를 참조하여 릴레이 테스트를 해 보시기 바랍니다.

7) 마지막으로

메일서버의 스팸 릴레이 차단기능만으로는 스팸메일에 대한 궁극적인 해결책은 될 수 없다. 다만 국내 정보통신망에서 운영되는 메일서버가 외부 악의의 사용자로부터 스팸메일 릴레이 서버로 악용되는 피해를 예방하는 차원에서는 상당히 좋은 기능이다.

스팸메일은 그 상업적인 가치로 인해 이와 관련된 서비스나 제품들이 많이 상용화 되어있으며 결과적으로 스팸메일이 범람하게됨에 따라 ISP 및 사용자들의 반발이 거세지면서 사회적 문제로 부각되고 있다. 이메일 폭탄에 의한 공격은 기존의 법률로 충분히 처벌이 가능하므로 별다른 대책이 필요하지 않을 것이다. 그러나 아직은 미국등 선진국에서조차 스팸메일을 명확히 범죄행위로 규정하는 법률이 없으며 현재 관련 법안이 제출되어있는 상태이다. 현재로서 스팸메일을 통제할 수 있는 법률적인 장치가 없기 때문에 각 ISP별로 사용약관 등을 이용하여 억제하고 있을 뿐이다. 이에 더해 전자우편 폭탄과는 달리 스팸메일은 그 상업적인 가치가 크기 때문에 사업자들의 입장과 사용자 및 ISP들의 입장이 상반되어 있다.

우리나라도 인터넷을 통한 산업의 육성과 사용자의 보호라는 모순을 잘 조화시키는 방향으로 스팸 전자우편이나 전자우편 폭탄 등을 포함하여 모든 정보시스템 오남용에 대한 제도적인 대책을 하루속히 마련하여야 할 것이다.

※ 참조 사이트

http://www.sendmail.org/tips/relaying.html
http://www.plus.or.kr/document/etc/sendmail.html
http://kldp.org/KoreanDoc/html/Sendmail-KLDP/Sendmail-KLDP-6.html
http://www.ntfaq.co.kr/emwac/view.asp?pid=12
http://www.microsoft.com/korea/technet/security/current.asp
http://kldp.org/~eunjea/qmail_relay.php
http://www.certcc.or.kr/paper/tr2001/tr2001-03/email security by procmail.html
http://www.microsoft.com/korea/exchange/default.asp
http://www.hyuks911.com/