

제목 : Mercury/32 에서 스팸메일 방지[Management]

Window 2000 Server 에서 Mercury Mail Server 스팸메일 방지 방안에 대해서 이야기 하고자 합니다.

아래 자료는 국내 “Mercury Mail Server” 을 활성화 시키고자 NTFAQ 회원이신 정상목씨가 제공 해 주신 문서입니다. 이번 주제는 “스팸방지, 릴레이방지”이며 마지막 진행 강좌 입니다.

작성자 : 정상목 (drcom@drcom.knue.ac.kr) , <http://drcom.knue.ac.kr>

설치 작업 후 그외 문제가 되었거나 질문은 게시판을 활용 해 주시길 바라며, 사용 후 좋은 후기 또한 소개 시켜 주십시오

말씀 드렸드시피 Mercury/32 에서 스팸메일 방지하는 법을 한번 소개 하겠다. 새삼스럽게 스팸의 정의는 생략하겠다. 이 글을 읽는 분들은 이미 그 정도의 지식은 다 알고 계시리라 믿고. 스팸을 차단하는 방법은 크게 2 가지가 있다. Server side 나 아니면 Client side 나에 따라서 다르다. 각각을 살펴보고 설정 방법을 알아 보기로 하자.

1. Server Side Spam 방지.

첫 번째 방법은 메일 서버 쪽에서 들어오는 Spam 을 차단하여 최대한 원하지 않은 메일을 걸러 내는 것이다. Mercury 에서는 크게 2 가지 방법을 제공해 주고 있다. Maps RBL 모드와 ORBS 모드가 있다. 두 가지 모드가 있기는 하지만 Mercury 를 만든 제작자도 말했듯이 두 가지 스팸 Control 을 제공해 준다고 해서 완전치 믿지는 말아 달라는 당부도 있다.

두 번째 방법은 Filtering 방법이다. Filtering 은 내용기반으로 동작한다. 들어오는 메일의 헤더, 혹은 body 나 등 메일의 내용을 사용자의 정의에 따라서 수신자에게 도달 하기 전에 AutoFowarding 할 수도 있고 Delete 할 수 도 있다.

(1) Mercury/32 에서 제공해 주는 Spam Control 에 대해서 알아보겠다. 별다른 매뉴얼이 없어서 제공해주는 Help 파일을 참고하였다.

먼저 당부의 글을 요약해 보면

1. 모든 스팸을 잡을 수는 없다. 이러한 Spam Control 기능이 당신 Site 에 들어오는 모든 메일을 예방할 것이라고 단순히 믿지 마라. 이러한 기능은 당신이 스팸 메일을 받을 수 있는 단계를 낮추는 것이다. 좀더 강한 Spam 차단 방법을 알아보려면 <http://www.cauce.org> 로 접속해서 스팸메일과 한판 붙을 방법에 관한 Overview 를 참고하라.

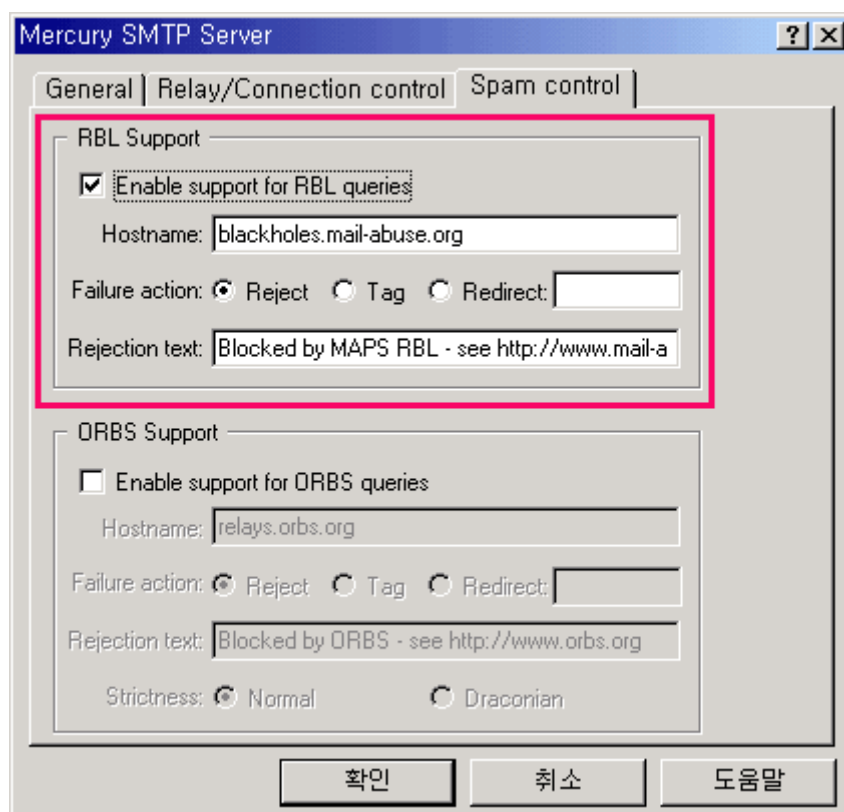
2. 때때로 정당한 메일이 스팸메일로 오인이 되어 차단되는 경우가 있다. 그 점에 대해서는 책임 못진다.

따라서 이러한 Spam Control 을 사용할 때는 조심스럽게 사용해야 하며 위험이 도사리고 있다는 것을 생각해 두어야 한다.

라고 떠들고 있다. 위험이 있던 말던 어쨌거나 이러한 위험을 감수하고 스팸을 차단하는 방법에는 크게 MAPS RBL Support 와 ORBS Support 가 있다.

MAPS RBL Support : Internet DNS 의 아버지라 불리는 Paul Vixie 가 운영하는 데이터베이스이다. 이 사이트에서는 스팸메일에 관한 사이트라든지, 상업성 **스팸에** 관한 리스트를 데이터베이스화 하고 있다. 만약에 RBL 데이터 베이스에 있는 리스트에 해당하는 사항이 있는 메일이 접속을 **하게되면** Mercury 는 알려준다. 자세한 사항은 <http://www.mail-abuse.org> 로 접속해서 알아보라.

다음 그림은 RBL 설정 그림이다. Configuration -> Mercury SMTP server -> Spam control 탭을 누르면 다음과 같은 그림이 나온다.

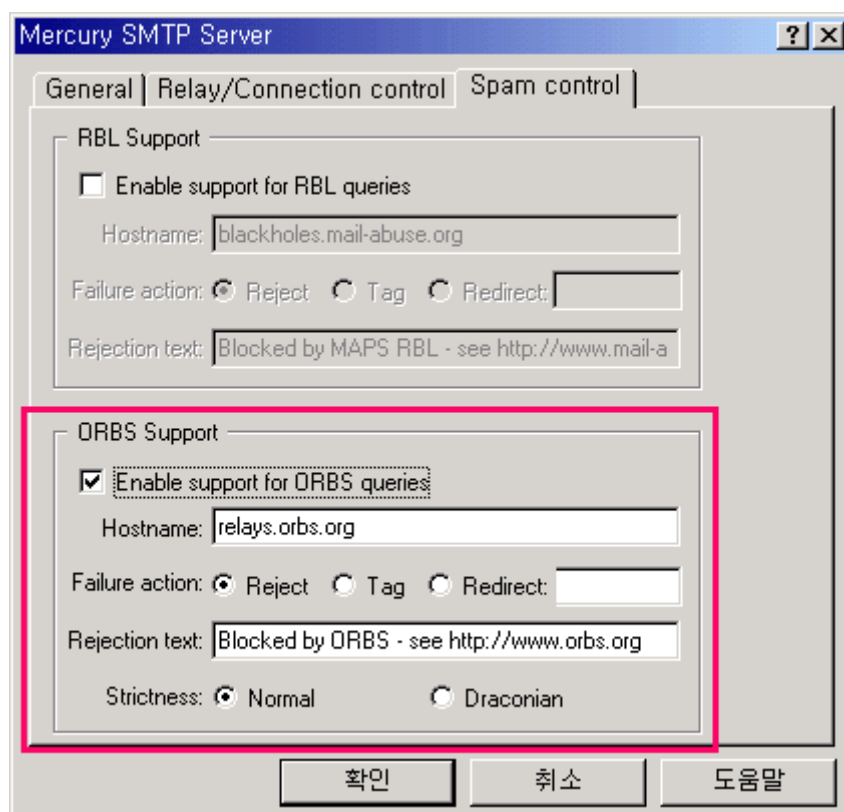


Hostname : RBL 데이터베이스를 사용할 도메인을 적어 주는 곳이다. 조심해야 할 것은 MAPS RSS 서비스를 사용하고 있거나 MAPS RBL+서비스를 사용하고 있다면 Hostname 에 그 서비스를 제공하는 곳의 도메인을 적어준다.

Failure action : RBL 리스트에 있는 곳으로부터 메일이 날아 왔을 때 어떻게 하겠느냐에 대한 설정이다. Reject 는 완전히 접근 거부로 설정하는 것이고 tag 나 Redirect 는 오른쪽 공란에 적어주는 주소로 메일을 보내 버린다는 것이다. 메일주소는 Nonlocal 이든지 Local 이든지 상관없이 48 장 정도의 주소를 적어 주면 된다. tag 는 헤더에 "X-RBX-BLOCKED"라는 메시지를 추가한다. 이점이 Redirect 와는 다른 점인데 별 효과 없는 방법이다.

Rejection text : 메시지가 RBL 에 적중했기 때문에 Rejected 하였다고 알려주는 난이다. 최대 80 자까지 가능하다.

다음은 ORBS Support 에 대한 그림이다.



Site 중심적인 RBL 비하여 ORBS 는 Open relay 방식을 사용한다. 즉 모든 메일에 대하여 로컬 사용자가 아니더라도 받아들이고 통과 시킨다. Open relay 는 인터넷 상에서 common practice 를 사용해야 하지만 스팸머들의 메일전송의 남용으로 인하여 사용되고 있어 지금은 거의 포기한 상태이다. 여기서 중요하게 알아 두어야 할 점은 ORBS 가 모든 스팸머들의 메일전송에 책임이 없다는 것을 의미하지는 않는다는 것이다. ORBS 는 좀더 정책적인 기관이다. 좀더 자세한 정보를 알고 싶으면 <http://www.orbs.org> 로 접속하라.

설정방법은 RBL support 와 유사하다. 다른 점은 다음과 같다.

Hostname : 일반적인 값으로 relays.orbs.org 를 적는다.

Tagging : 헤더에 "X-RBX-BLOCKED"라는 메시지를 추가하여 보낸다.

이점이 Redirect 와는 다른 점인데 별 효과 없는 방법이다.

Strictness : 기본값으로 Normal 을 사용한다. Draconian 는 모든 ORBS 에서 오는 어떠한 Mail 이라도 fail 한다.

이상으로 스팸컨트롤을 살펴 보았다. 경험상 아직 다양한 방식의 스팸을 받은 경험이 없더라도 여러 가지 방식의 제어는 다루어보지 못했다. 하지만 RBL 과 ORBS 를 적절히 사용한다면 절대적으로 스팸을 차단 할 수는 없지만 어느 정도는 downsizing 하리라 본다.

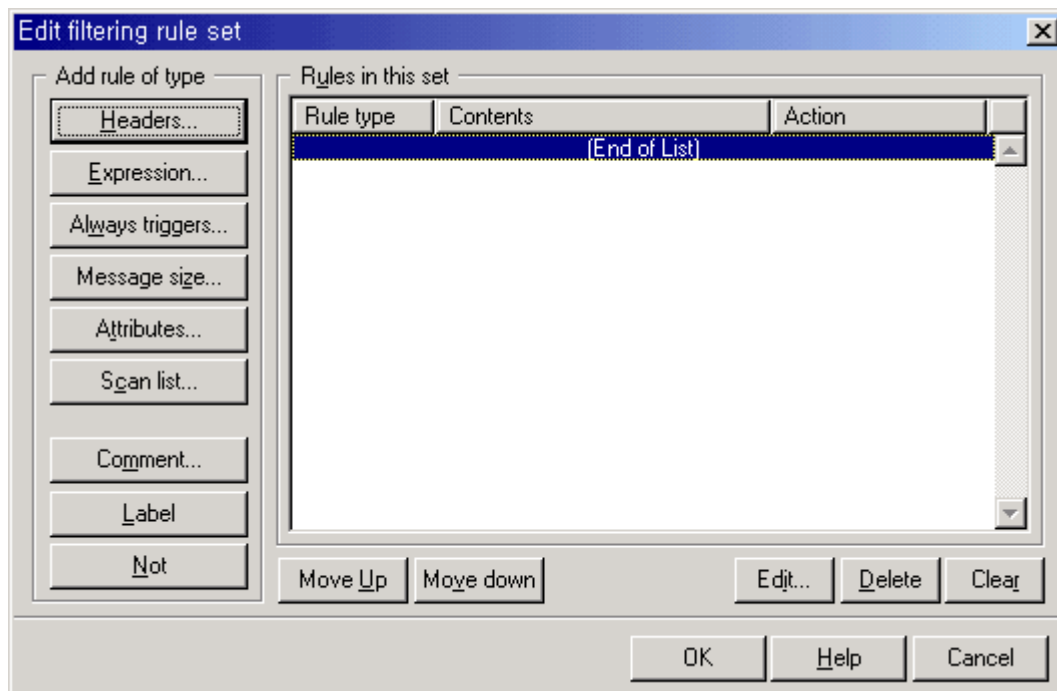
하지만 제작자 당부에 말에서도 밝혔듯이 정당한 메일이 스팸메일로 오인되어 차단되는 경우도 생길 수 있다.

본 내용을 보고 "뭘 도대체 어떻게 하라는 거야? 하라는 거야. 말라는 거야?"라는 생각도 들 것이다. 구체적인 제시는 하지 않겠다. 내용을 보고 사용자가 판단하기를 바랄 뿐이다. 그만큼 조심스러운 부분이다.

(2) Filtering 기법

메일의 내용 중 사용자가 제시한 제어 단어와 일치 여부에 따라 다양한 Method가 지원된다. 다량의 메일을 처리함에 있어서 필터링을 거쳐 메일이 수신되기 때문에 메일 서버에 대한 오버헤드는 존재한다. 그러나 설정도 까다롭지 않으며 간편하다. 필자도 아직까지 모든 옵션을 사용해 보지는 못했다. 모든 경우와 조건에 따른 예시를 제시해 주었으면 하는 바램이지만 매뉴얼도 없고 참고할 만한 자료가 없으므로 많이 사용하는 방법을 중심으로 설명하고자 한다.

Configuration -> Filtering rules -> Edit global rules 를 누르면 다음과 같은 화면을 볼 수 있다.



Edit filtering rule set 은 내부 들어오는 메일과 외부로 나가는 모든 메일에 대해서 필터링이 적용된다. 왼쪽 메뉴를 보면 적용 rule 에 대한 버튼이 있다. 가장 많이 사용하는 것이 Headers...라는 버튼이다. 예를 하나 들어 설명해보기로 하자.

[제임스씨는 잦은 출장을 한다. 따라서 자리를 비우는 경우가 많다.

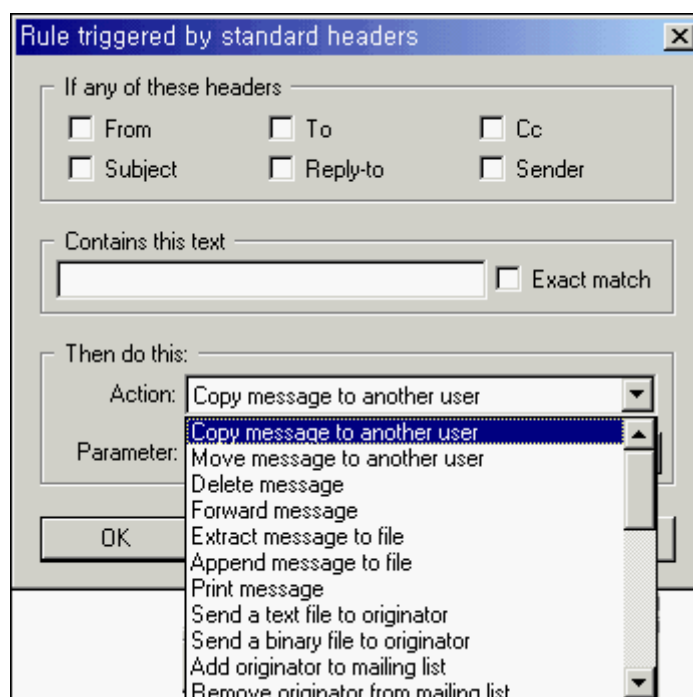
okebari@yes.no.kr 로부터 메일을 급히 받아야 한다. 메일을 받으려면 외부에서 POP3 를 이용하여 받을 수 있다(외부 메일 주소는 yesbari@ok.no.ac.kr 이다). 하지만 메일서버에 카피본 한부를 두어 사무실에도 메일을 보고 외부에서도 메일을 한부 받고자 한다. 어떤 방식을 사용하면 될까?]

Mercury/32 에서도 이러한 기능을 지원하고 있다. 바로 Action 이라는 부분이다. 굉장히 다양한 Action 이 존재한다. 예시를 중심으로 설명하며 해결하기로 하자.

먼저 Headers...이라는 버튼을 클릭한다. 다음과 같은 그림이 나올 것이다.



If any of these headers 라는 부분은 메일의 헤더를 검색하여 Contains this text 라는 부분과 검색하여 match 되는 부분이 있으면 Then do this 하라는 명령이다. 아까 예시를 설정해보면 okebari@yes.no.kr 로 부터 메일이 오므로 From 부분을 체크해주고 Contais this text 부분에 okebari@yes.no.kr 라고 적어준다. Action 을 보면 Copy message to another user 가 보인다. 오른쪽 콤보 버튼을 눌러 보면 다양한 Action 이 존재 함을 볼 수 있다.



먼저 간단히 소개를 하겠다. 필자도 다 써보지는 않았다. 주로 많이 사용하는 Action 을 중심으로 설명하겠다.

[Copy message to another user](#) : 다른 로컬 사용자에게 복사해서 보낸다. 원본은 그대로 있고 카피본만 보낸다.

[Move message to another user](#) : 다른 로컬 사용자에게 이동 시킨다. 원본을 그대로 이동 시킨다.

[Delete message](#) : 메일을 삭제해 버린다.

[Forward message](#) : 메일을 Forwarding 시킨다. 중요한 점 원본은 서버에 남아있으며 복사본만 Forward 시킨다.

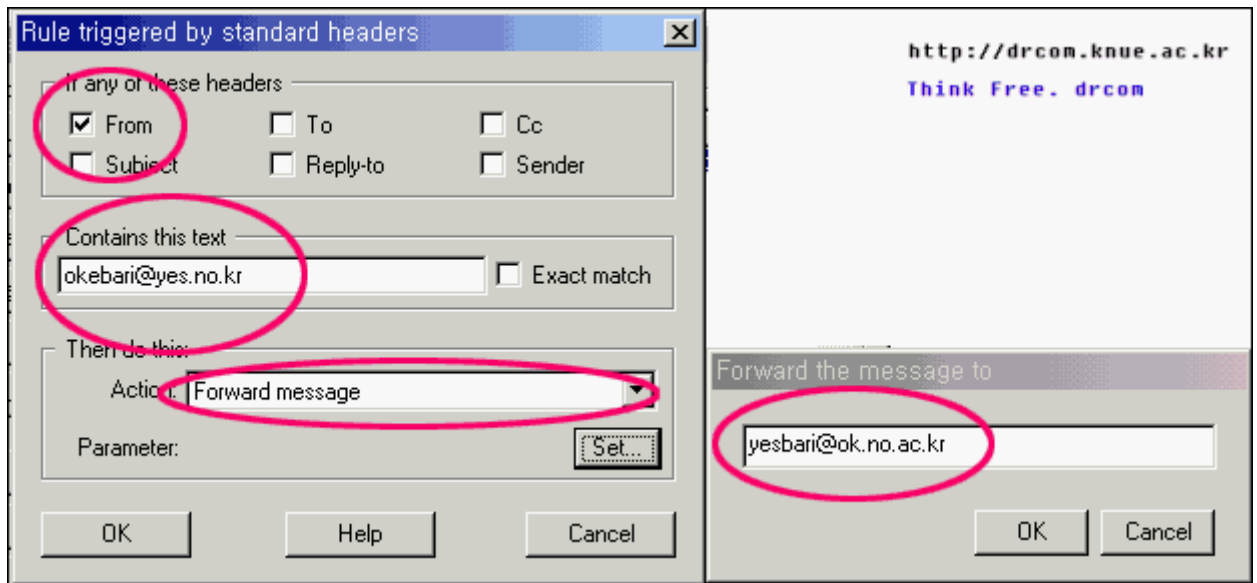
[Extract message to file](#) : 메일에서 첨부파일만 추출한다.

[Append message to file](#) : 메일에 파일을 첨부시킨다.

[Print message](#) : 메일이 오면 출력한다.

...

나머지는 Action 은 나름대로 의미를 파악하고 각자 사용해보도록 한다. 그러면 제시한 문제를 해결하려면 원본은 메일 서버에 있어야 하므로 Action Forward message 를 선택하고 set 버튼을 눌러 받을 메일 주소를 입력한다. yesbari@ok.no.ac.kr 를 적는다. 완성된 그림이 다음과 같다.



흐뭇하지 않은가? 흐뭇~~~. 이렇게 설정해 놓으면 메일 서버에 원본이 있으므로 나중에 사무실에서 접속해서 받아 볼 수도 있으며 원격지에서도 POP3 를 지원하므로 메일을 받아 볼 수가 있다.

갑자기 이런 의문이 든다. 그러면 Forward message 하고 Copy message to another user 하고의 차이점은? 그것은 간단히 생각해 볼 수 있다. Forward message 는 말 그대로 메일 Forwarding 을 해주는 것이고 Copy message to another user 는 로컬 유저에게 메일을 보내는 것이다. Forward message 에서 set 을 로컬 사용자의 메일 주소로 적는 것과 같은 의미이다. 유심히 보아야 할 Action 이 있다. 바로 **Delete message** 이다. 이 부분에서 적당히 필터링을 하여 스팸메일을 삭제하면 스팸메일을 차단 할 수 있을 것이다.

Headers...버튼 아래에 있는 것들은 단독적으로 동작하는 것은 아니다. Headers 와 연계하여 동작을 한다. 연계에 대한 구체적인 사항은 언급하지 않겠다. 나름대로 연계하여 사용해 보기를 권장한다.

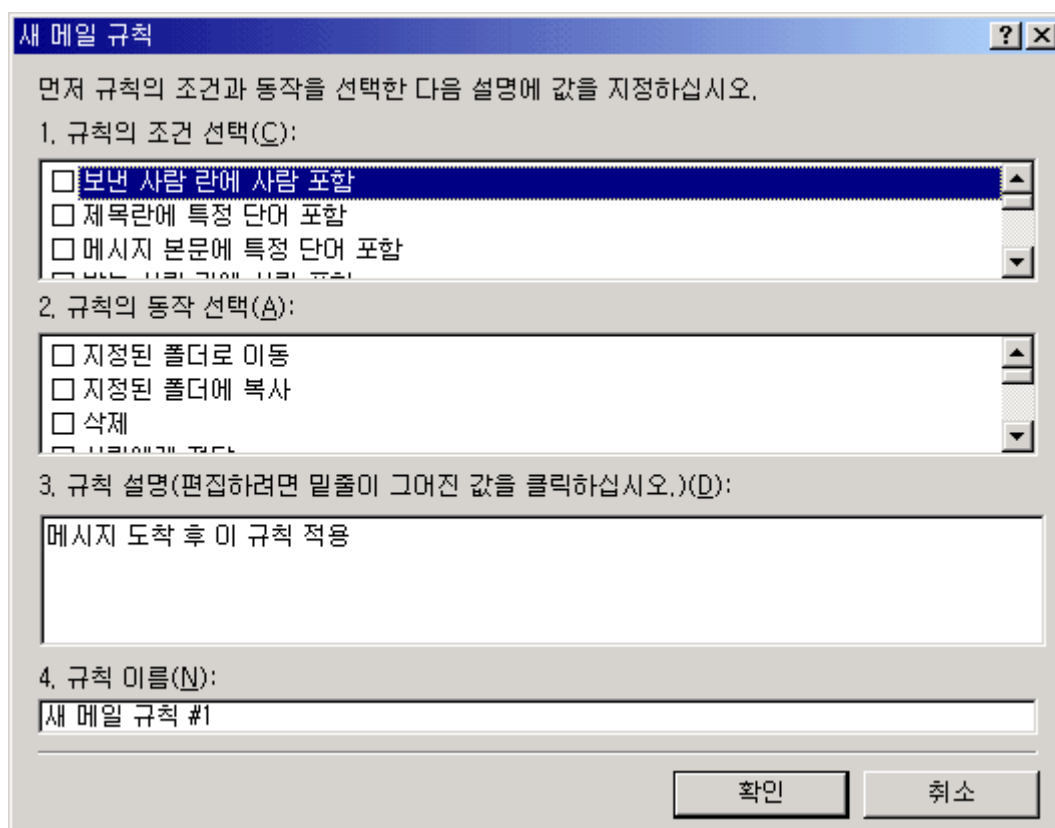
2. Client Side Spam 방지.

Client Side Spam 방지는 메일서버에서 필터링 하지 못한 부분을 Client 에서 제어 해 주는 부분이다. 즉 사용자의 구성에 맞게 필터링을 하는 부분이다. 사실 메일 관리자는 스팸에 대한 1 차 책임은 있지만 모든 메일에 대한 통제는 어렵다. 즉 사용자가 원하는 메일인지 그렇지 않은 메일인지 구분이 어렵다는 것이다. 일반적으로 대량의 스팸 메일에 대해서는 관리자의 책임이지만 도착하는 메일의 하나하나의 선택여부는 개인이 선택을 해야만 한다.

요즈음에는 전자상거래법의 활성화에 따라 메일수신여부를 묻는 메일방식이 많아 지고 있다. 하지만 아직도 음란 CD 판매나 메일 수신여부가 없는 메일, 혹은 원하지 않은 메일을 계속해서 보내는 경우가 많다. 이럴 때 사용자는 관리자를 탓 하지 말고 사용 메일 프로그램에서 적절하게 필터링하여 원천 봉쇄할 수 있다.

말도 많고 탈도 많은 Out-Look express 를 중심으로 작성하겠다. 이를 선택한 이유는 아직도 많은 사용자가 Out-Look Express 를 사용하리라 생각이 들기 때문이다.

Out-Look Express 실행 -> 도구 -> 메시지규칙(R) -> 메일을 클릭한다.

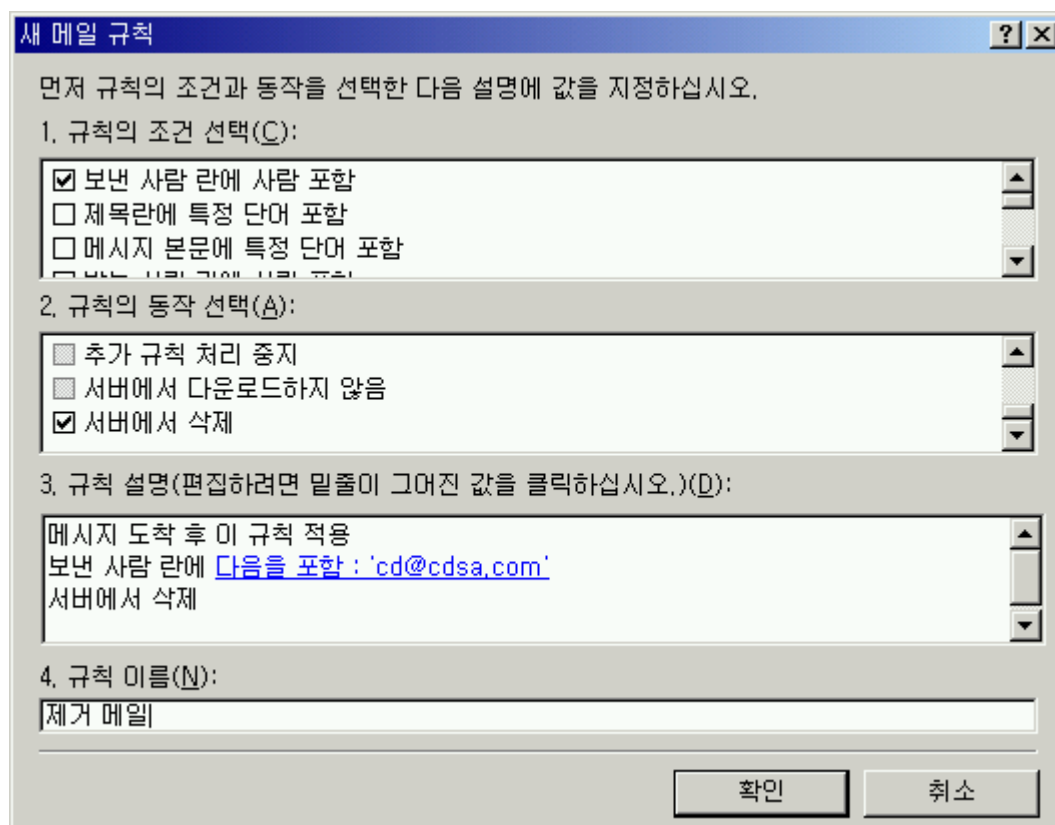


다양한 규칙 조건(1)이 있으며 규칙에 Match 가 되는 사항이 있으며 어떻게 하라는 규칙동작(2)이 있다. 이러한 규칙에 대한 세부사항은 규칙설명(3)에서 설정할 수 있다.

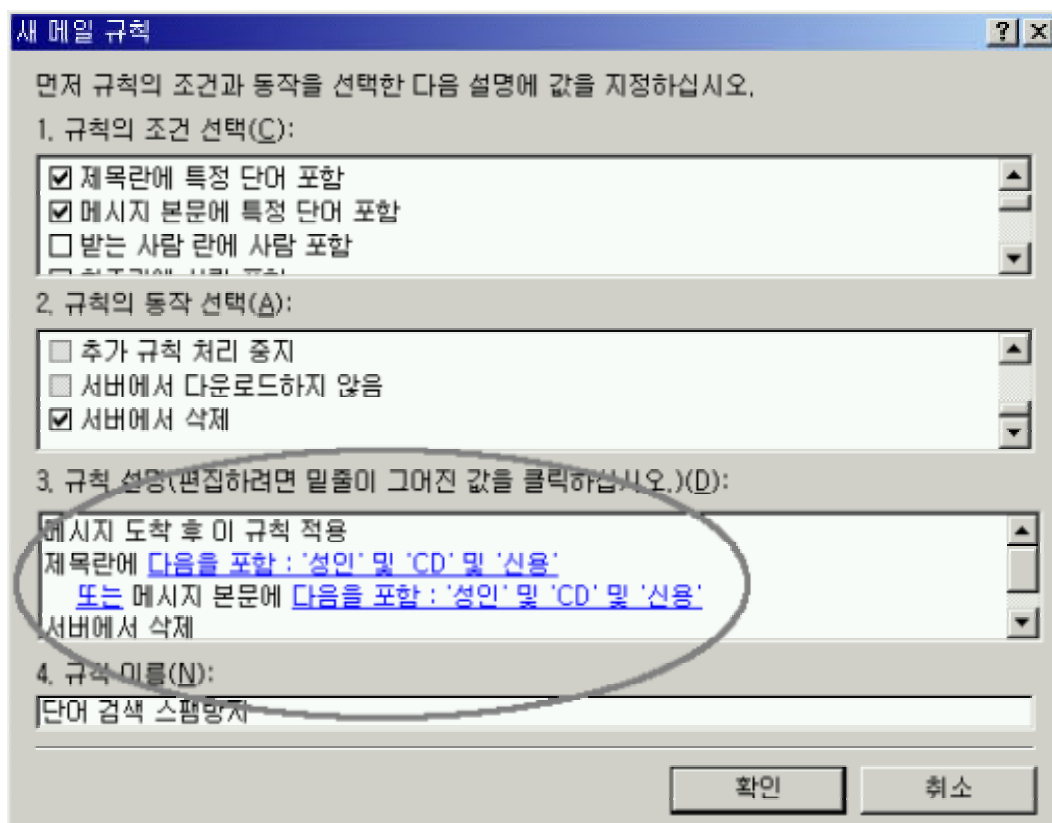
[제임스씨는 cd@cdsa.com 으로부터 음란 CD 를 사라는 메일을 하루에 20 통씩 받는다. 내용을 읽어 공통 단어를 보았더니 '성인', '신용', 'CD'란 말이 공통적으로 들어가 있다. 일일이 삭제하자니 신경질만 났다. 어떻게 삭제하는 방법이 없을까?]

본 drcom 기자와 제임스씨와의 인터뷰를 통해 많은 고충이 있음을 알 게 되었다. 그래서 drcom 기자는 해결 방법을 제시하였다.

먼저 보낸 사람을 명확히 알고 있으므로 보낸사람란에 포함을 체크한다. 메일을 읽을 필요조차 없으므로 삭제를 해야 되는데 2 가지 방법이 있다. 한가지는 메일서버에서 메일을 가져와서 삭제하는 방법이 있고 다른 방법은 메일 서버에서 아예 삭제해 버리는 방법이 있다. 그런 메일은 메일서버에서 가져올 가치가 없으므로 메일서버에서 삭제해 버릴 것이다. 규칙의 동작 선택은 맨 아래쪽에 서버에서 삭제를 선택한다. 그리고 나서 규칙 설명 중에 사람포함을 클릭하여 cd@cdsa.com 을 써준다. 완성된 그림이 다음과 같다.



그러나 이것만으로는 완벽하지 않다. 보통 스팸을 보낸 이의 메일 주소는 수시로 바뀌기 때문에 고정된 메일 주소를 지정하여 스팸을 방지한다는 것은 불가능 하기 때문이다. '성인', '신용', 'CD'란 말이 공통 적으로 들어갔기 때문에 제시된 문자열로 스팸을 방지해야 한다. 조심스러운 것은 절대 한 단어로만 필터링을 하지 말아 달라는 것이다. 적어도 3 개 이상의 단어를 Regular Expression 을 사용하여 필터링을 해야 위험이 적다. 다음 그림은 '성인', '신용', 'CD'란 단어를 가지고 스팸을 방지하는 그림이다.



규칙설명을 잘 보고 설정해야 한다. 무슨 내용인가 하면 제목란 혹은 메시지 본문에 '성인', 'CD', '신용'이란 3 단어가 일치 하였을 경우 서버에게 메일을 삭제 하라는 이야기 이다.

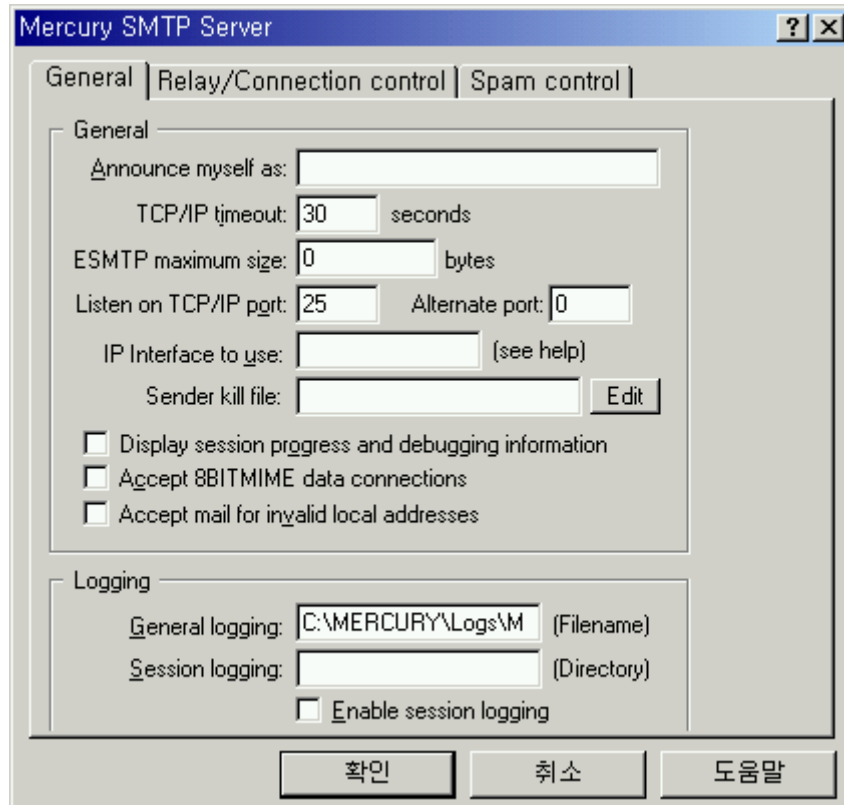
3. Spam Relay 방지.

필자가 소개에서 밝힌 바와 같이 스팸 릴리이 방지는 **무척 중요하다**. 늘 로그 파일을 분석하여 혹 나의 메일 서버가 릴레이 서버로 쓰이지 않는가를 분명히 파악해야 한다. 스팸 릴레이 방지는 생각 외로 무척 간단하다.

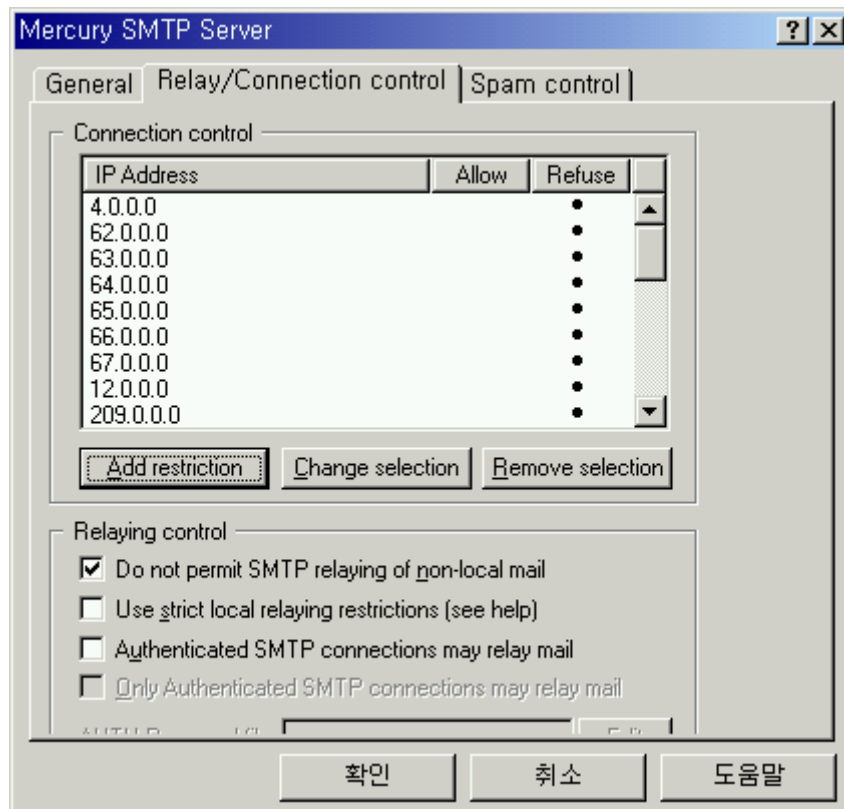
아주 아주 중요한 부분이다. 나 이거 때문에 정통부로부터 물먹은 적이 한번 있다. 이거 조심해야 한다. 미국쪽에서 특히 미국 야한 Site 운영하는 곳에서는 그러한 부분을 자주 발생을 야기 시킨다. 내 메일 서버를 가지고 스팸을 마구 뿌려 댄다. 내가 강조하는 부분이 이 부분이다. 처음에는 EMWAC 을 썼었다. 잘 썼다. 무척...근데 언젠가부터 쓰지도 않은 네트워크에 부하가 걸렸다. 잘 몰랐다. 그냥 ARP 가 도는가 하고 생각했었다. 근데 이러한 스팸 메일을 내 메일서버를 이용해서 메일을 막 보내더라는 것이다.

이제는 끝이다. 바로 릴레이 방지가 Mercury에 있기 때문이다. 더 이상 메일 릴레이를 할 수 없게 만들었다.

Configuration에 Mercury SMTP Server를 선택한다. 다음 그림과 같은 창이 나온다.



Relay/Connection control 탭을 누른다. 다음과 같은 창이 나온다.



보고 있는 것이 메일을 보내는 스팸머들의 주소들이다. 특히 미국에 있는 IP가 64.x.x.x로 시작하는 스팸머하고 65.x.x.x로 시작하는 스팸머들을 잘 보아두길 바란다. 이 스팸머들은 수시로 IP를 62.x.x.x, 63.x.x.x, 64.x.x.x, 65.x.x.x, 66.x.x.x 등으로 바꾸어 메일을 보낸다. 추적결과 동부에 있는 스팸머들인데, 아까 설치한 C:\WMERCURYWLOGS에 보면 자세한 로그파일이 있다.

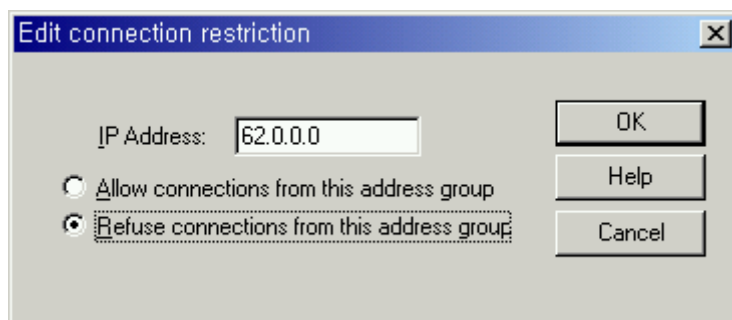
아래쪽에 있는 *Do not permit SMTP relaying of non-local mail*과 *Use strict local relaying restriction*을 설명하겠다. *Do not permit SMTP relaying of non-local mail*은 Help 파일을 참고해 설명해 보겠다.

Mercury/32는 모든 메일에 대하여 Accepted한다. 비록 로컬메일이 아니더라도 말이다. 주소가 맞지 않든지, 혹은 Local 메일이 아니든지 간에 Mercury/32는 모든 메일에 대해서 일단은 받아 놓는다. 그리고 나서 위의 그림에 나와있는 "allow"의 리스트를 참고하여 만약에 "allow" 항목에 없는 주소이면 "571 - Sorry, we do not relay non-local mail"이라는 메시지를 출력하고 메일을 서버에서 삭제한다. 따라서 스팸메일을 Control을 하려면 *Do not permit SMTP relaying of non-local mail*에 체크를 하고 내가 받고자 하는 상대방의 IP를 추가하고 반드시 "allow"로 추가시켜 놓아야 한다. 그렇지 않으면 스팸머들의 칭찬과 함께 스팸머들이 즐겨 쓰는 메일서버가 될 것이다. *Do not permit SMTP relaying of non-local mail*를 Normal Mode라 부른다.

다음 *Use strict local relaying restriction*은 Normal Mode의 모든 룰을 적용 받지만 메일을

보내는 이의 "From"의 주소를 참조하여 List 에 나와 있는 "allow"를 비교하여 메일 송수신여부를 결정한다.

Add restriction 을 누른다. 해당 IP 를 넣는다. 예를 들어 62.0.0.0 이라고 쓰면 62 로 시작하는 IP 는 다 거부해 버린다. 즉 62.0.0.0 부터 62.255.255.255 까지 막아 버린다는 것이다. 다음 그림은 62.0.0.0 을 추가시키는 그림이다.



이런식으로 다음 A class IP 를 잔뜩 추가 시킨다. 반드시 추가 시킬 IP 는 다음과 같다.

- 4.0.0.0
- 24.0.0.0
- 62.0.0.0
- 63.0.0.0
- 64.0.0.0
- 65.0.0.0
- 66.0.0.0
- 67.0.0.0
- 68.0.0.0
- 69.0.0.0
- 209.0.0.0
- 216.0.0.0

참고로 61.0.0.0 은 막지 않을 것. 우리나라에 할당된 IP 이다. 우리나라에 할당된 IP 를 보려면 <http://domain.nic.or.kr/> 로 접속해서 확인해 보기바란다.

이상으로 Mercury 에 대한 설정을 마친다. 얼마나 IP 를 바꾸어 가면 현란하게 접속하려 하는가?

```
E 20011127 000917 0 Connection from 65.44.224.46 refused because of restriction.  
E 20011127 001733 0 Connection from 65.44.224.46 refused because of restriction.  
E 20011127 002232 0 Connection from 65.44.224.24 refused because of restriction.
```

E 20011127 004303 0 Connection from [65.44.224.44](#) refused because of restriction.
E 20011127 004557 0 Connection from 65.44.224.44 refused because of restriction.
E 20011127 004902 0 Connection from 65.44.224.44 refused because of restriction.
E 20011127 010941 0 Connection from [65.44.224.49](#) refused because of restriction.
E 20011127 012230 0 Connection from [65.44.224.42](#) refused because of restriction.
E 20011127 012928 0 Connection from 65.44.224.42 refused because of restriction.
E 20011127 013421 0 Connection from 65.44.224.42 refused because of restriction.
E 20011127 013712 0 Connection from 65.44.224.42 refused because of restriction.
E 20011127 014027 0 Connection from 65.44.224.42 refused because of restriction.
E 20011127 021951 0 Connection from [65.44.224.80](#) refused because of restriction.
E 20011127 022107 0 Connection from 65.44.224.80 refused because of restriction.
E 20011127 022618 0 Connection from 65.44.224.80 refused because of restriction.
E 20011127 023248 0 Connection from [65.44.224.57](#) refused because of restriction.

문제가 생겼다. 나는 미국과 자주 E-mail 을 왕래한다. IP 를 모두 restriction 시켜서 어떻게 하는가? 답은 쉽다. 예를 들어 미국의 메일 서버가 65.44.225.7 라면 Configuration 에 Mercury SMTP Server 에서 Configuration 에 Mercury SMTP Server 탭을 선택하고 65.44.225.7 를 써주고 Allow connection from this address group 을 선택하면 해당 서버의 메일을 받을 수 있다.

이상으로 스팸방지에 대한 다양한 방법을 제시해 보았다.

