

스팸릴레이 방지관련 업체별 보안패치

□ 탑플래시 (www.i-top.biz)

버전에 따라 방화벽설정변경해야함

o 버전 1.x의 패치프로그램 : flashpatch-22

o 버전 2.x의 패치프로그램 : toproxy-15

1. 탑플래시 1.x의 경우

① 웹서버에 루트(root)계정으로 로그인한다.

② 아래 명령어를 사용하여 탑플래시의 설정화일이 있는 디렉토리로 이동한다.

```
cd /usr/local/topflash/conf
```

③ conf 디렉토리에서 “filter.conf” 파일을 vi에디터로 불러낸다.

```
vi filter.conf
```

④ 파일의 내용중 아래 내용을 찾아서 그 줄을 삭제한다.

```
0.0.0.0/0 -> '탑플래시가 설치된 서버 IP'
```

해당 줄을 찾으면 ‘dd’를 눌러서 삭제한다.

⑤ ‘:’를 누룬후 ‘wq!’를 타이핑한다.

⑥ 탑플래시를 재실행한다.

2. 탑플래시 2.x의 경우

① 웹서버에 루트(root)계정으로 로그인한다.

② 아래 명령어를 사용하여 탑플래시의 설정화일이 있는 디렉토리로 이동한다.

```
cd /usr/local/topflash2/conf
```

③ conf 디렉토리에서 “firewall.conf” 파일을 vi에디터로 불러낸다.

```
vi firewall.conf
```

④ 파일의 내용중 아래 내용을 찾아서 그 줄을 삭제한다.

```
TCP 0.0.0.0/0 sport:* => 0.0.0.0/0 dport:* => ALLOW  
TCP 0.0.0.0/0 sport:* => 0.0.0.0/0 dport:* => LOGNALLOW  
TCP 0.0.0.0/0 sport:* => 0.0.0.0/0 dport:8080 => ALLOW  
TCP 0.0.0.0/0 sport:* => 0.0.0.0/0 dport:8080 => LOGNALLOW
```

해당 줄을 찾으면 ‘dd’를 눌러서 삭제한다.

- ⑤ ‘:’를 누른 후 ‘wq!’를 타이핑 한다.
- ⑥ 탑플래시를 재실행 한다.

□ 보라매 (www.desicom.co.kr)

- ① “www.desicom.co.kr” 사이트로 이동
- ② 홈페이지 좌측 하단의 [다운로드] 메뉴를 클릭
- ③ 20번 제목 “안티스팸 적용 버전 Sendmail cf doc”에서 “Sendmail”을 클릭
- ④ sendmail-8.12.2-11.i386.rpm 패치 프로그램 다운로드
- ⑤ 새로 설치할 경우에는 아래 명령어를 사용

```
rpm -i sendmail-8.12.2-11.i386.rpm
```

- ⑥ 옛날 버전을 새로나온 버전으로 업데이트 하려면 아래 명령어 사용

```
rpm -Uvh sendmail-8.12.2-11.i386.rpm
```

- ⑦ 보라매를 재실행 한다.

□ 포트라 (www.portra.com)

포트라에서의 메일릴레이 방지는 다음 두 가지 경우에 따라 서로 다른 절차로 이루어져야 한다.

1. 메일서버를 사용하지 않는 경우

- ① telnet 접속

```
<telnet 접속방법>  
telnet 서버아이피  
Password:1차 패스워드입력  
portra> en  
Password:2차 패스워드입력  
portra# reload Shell
```

- ② sendmail 데몬의 모드를 변경해 준다.

```
<모드 변경방법>
```

```
cd /etc/rc.d/init.d/  
chmod 000 sendmail
```

2. 메일 서버를 사용할 경우

- ① telnet 접속
- ② /etc/sendmail.cf 편집으로 RELAYING DENY 시킴.

< RELAYING DENY 방법 >

vi /etc/sendmail.cf 엔터

찾은 윗부분에서 아래와 같은 문자열을 확인한다.

anything else is bogus

R\$* \$@ OK

이것을 아래와 같이 수정한다.

anything else is bogus

#R\$* \$@ OK

R\$* \$#error \$@ 5.7.1 \$: "550 Relaying
denied"

- ③ 저장 후 vi 편집기를 빠져나와 샌드메일 데몬을 재실행 시킨다.

/etc/rc.d/init.d/sendmail restart

- ④ /etc/mail/access 파일을 편집해서 내부아이피들은 RELAYING 을 허용 시킨다.

ifconfig 로 내부 아이피 대역 확인

(ex) eth0: 100.10.10.1 , eth1: 192.168.1.10 , eth2: 192.168.2.10

vi /etc/mail/access 엔터

파일 맨아래에 위의 아이피 대역들을 RELAY 시킨다.

100.10.10 RELAY

192.168.1 RELAY

192.168.2 RELAY

저장 후 빠져 나온다.

- ⑤ 아래의 방법으로 파일 실행시켜 줌.

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

□ 썬더웹 (www.netfree.co.kr)

- ① “www.netfree.co.kr”사이트로 이동
- ② 홈페이지 우측상단의 [자료실]메뉴 클릭



- ③ 번호 20번 제목 “[썬더웹프록시]프록시 보안문제 패치프로그램” 클릭
- ④ patchacl 다운로드
- ⑤ 위 패치프로그램을 웹서버에 설치한후 다음처럼 설정한다.

```
# chmod 755 patchacl
# ./patchacl
# /etc/rc.d/init.d/ThunderWeb restart
```