프락시 서버를 이용한 인터넷 주소 세탁

정현철 선임연구원 hcjung@certcc.or.kr
오규철 연구원 kcoh@certcc.or.kr

1. 개요

기업의 비자금이나 탈세 자금 등의 검은돈을 다른 계좌에 여러 차례 넣었다 뺐다 하는 등의 수법으로 자금 출처의 추적을 어렵게 하는 일을 “돈세탁(Money Laundering)"이라고 한다. 그런데, 사이버 공간에서도 타 시스템에 대한 불법적인 침입, 대량의 광고성 메일 발송 등 불법적인 목적으로 인터넷을 사용할 때 자신의 인터넷 주소(IP)를 세탁함으로써 추적을 어렵게하는 일들이 심심치 않게 발생되고 있다.

인터넷을 불법적인 목적으로 사용하고자 하는 이들은 웹 프락시 서버, 캐쉬 서버, 심지어는 애플리케이션 Firewall까지 인터넷 주소 세탁에 이용하고 있다.

이러한 프락시 서버를 이용하여 타 시스템에 침입하거나 스팸 메일을 발송하였을 경우 공격을 당한 사람이나 메일 수신자는 프락시 서버의 주소가 최초의 출처인 것처럼 오인하고 실제 공격자 또는 메일 발송자는 전혀 알수가 없다.

프락시 서버를 이용한 인터넷 주소 세탁은 기존의 해킹 경유지와는 달리 실제 시스템을 해킹하여 침투할 필요도 없다. 프락시 서버의 설정상의 오류를 이용하여 손쉽게 마치 프락시 서버에서 공격한 것처럼 보이게 할 수 있다.

앞서 언급한바와 같이 프락시 서비스는 캐쉬 서버, Firewall 등 광범위한 목적으로 사용되고 있으며, 이들 중 상당수에 임의의 TCP 접속을 연결해 줄 수 있는 취약점이 존재한다.

CERTCC-KR에 국내 프락시 서버를 이용한 스팸메일 발송에 대한 국외의 항의메일들이 빗발치고 있다. 각급 기관에서 운영중인 프락시 서버가 인터넷 주소 세탁에 악용되고 있는지 점검해 볼 필요가 있다.

본 고에서는 프락시 서버를 이용한 공격의 형태 및 사례 그리고 이를 방어하기 위한 방법에 대해 알아보기로 한다.

2. 프락시란?

문제가 되고 있는 프락시 자체에 대해서 간단히 살펴보도록 하자.

프락시(Proxy)는 대리자, 대행자로 해석되어 질 수 있는데 프락시 서버가 설정되어 있을 경우 우리가 어떤 웹 사이트에 접속할 때 곧바로 그 사이트로 가지 않고, 프락시 서버를 경유해서 가게 된다. 즉, 먼저 프락시 서버로 가서 프락시 서버에서 해당 웹사이트로 가게 된다. 새로운 웹 페이지를 방문할 때마다 프락시 서버에 저장이 되어 진다.

프락시 서비스를 사용하는 이유는 몇가지가 있을 수 있다.

첫째, 캐쉬(Cache) 서버로써 프락시를 이용할 수 있다. 캐쉬서버는 네트워크 트래픽 오버로드를 줄이고, 사용자들이 웹 서핑하는 속도를 빠르게 하기 위해서 프락시를 사용한다. 방문하고자 하는 사이트보다 프락시 서버가 가까이 있으면 서핑 속도도 빨라지기 마련이다.

둘째, 웹 컨텐츠 필터링을 위해서 사용할 수 있다. 실제 국내 대부분의 초중고교의 서버에는 음란물 차단을 위해 프락시 서버를 운영하고 있다.

셋째, 보안상의 목적으로 Firewall 등에서 사용할 수 있다. 실제 서버에 접속하기 이전에 애플리케이션 레벨에서 인증, 접근통제, 명령어 필터링 등을 수행할 수 있도록 프락시 서버를 사용한다.

이외에도 다양한 목적으로 프락시 서비스가 사용되어 질 수 있으며, 구현되어 판매되고 있는 제품 또한 대단히 다양하다.

3. 프락시를 이용한 공격 기법

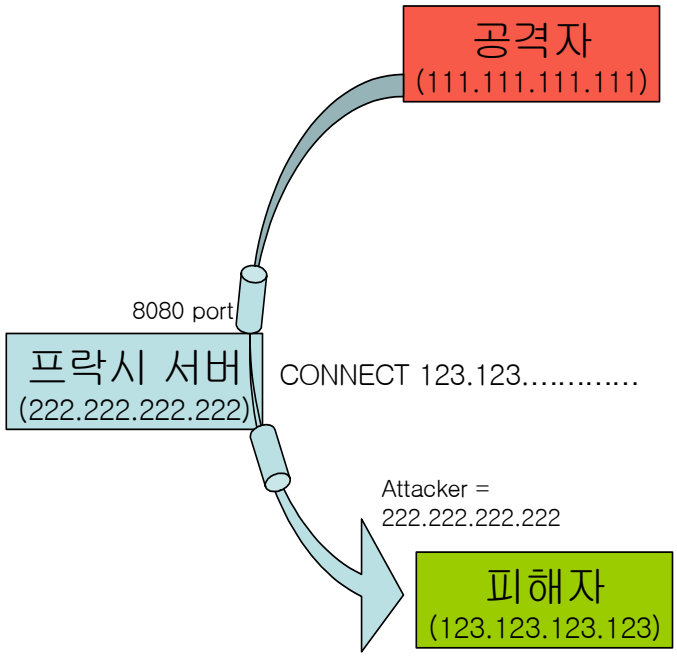
다양한 업체의 HTTP 프락시 서비스들은 보안이 고려되지 않은 default 설정 상태로 운영되고 있어 공격자가 내부 호스트나 외부 기관의 호스트에 임의로 TCP 접속을 맺을 수 있도록 하고 있다.

HTTP 프락시 서버들은 대개 TCP 연결을 할 수 있도록 설계된 HTTP CONNECT 방법을 지원해 주고 있다. 일반적으로 HTTP CONNECT 방법은 HTTP프락시를 통해서 HTTPS(443 port) 터널링에 사용된다. 프락시 서비스는 TLS/SSL에서 사용하는 단대단(end-to-end) 보안 모델을 위배하지 않기 위해 HTTPS 트래픽을 복호화하지 않는다.

HTTP CONNECT 방법은 이처럼 필요에 의해서 HTTPS, SNEWS와 같이 반드시 필요한 포트에 대해서만 제한하여야 한다.
하지만 많은 업체의 HTTP프락시 서비스는 모든 인터페이스에서 리슨하고 또한 모든 TCP 포트로 HTTP CONNECT 방법을 이용하여 접속을 맺을 수 있도록 default 설정되어 있다.

공격자들은 HTTP CONNECT 방법을 이용하여 telnet(23/tcp), SMTP(25/tcp)를 비롯하여 rlogin, rexec 등 다양한 서비스에 자신의 출처를 숨기고서 접속하고자 한다. 특히 SMTP에 대한 접속을 허용하도록 설정되어 있을 경우 스팸메일 발송에 사용되는 경우가 많다.
프락시 서버들, 웹 서버들, 캐쉬 서버들, Firewall, 그리고 Virus Wall과 같은 컨텐츠 필터링 제품들도 HTTP 프락시 서비스를 제공하고 있다. 또한, HTTP 프락시 서비스가 제공되는 포트도 제품마다 다양한데, 주로 80, 81, 1080, 8080, 3128, 8888 등의 포트가 많이 사용된다.

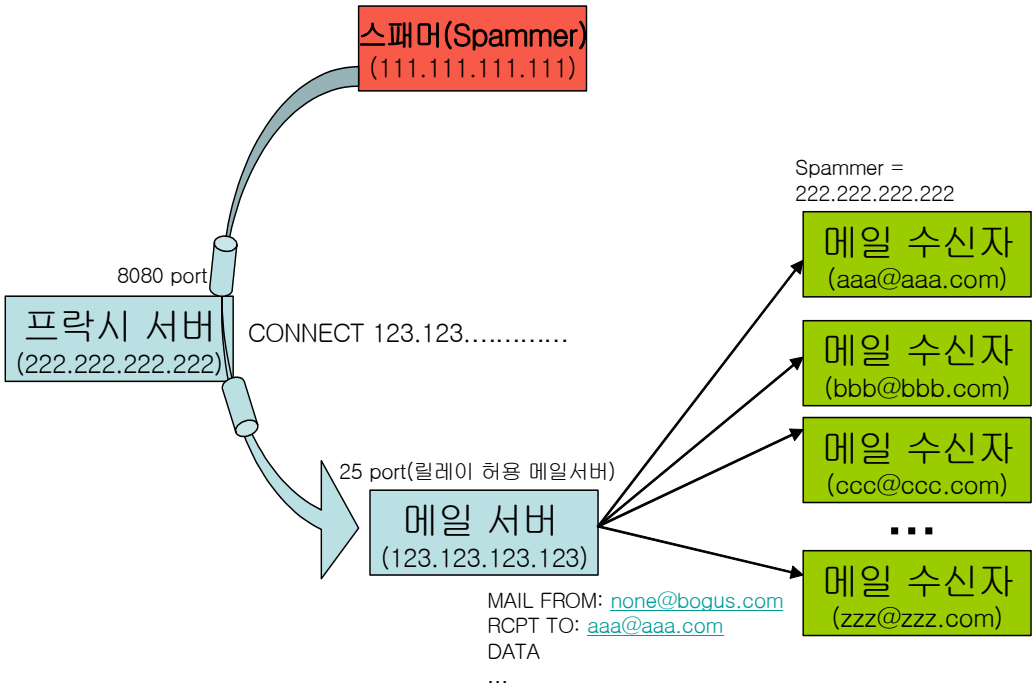
(그림 1)은 공격자(111.111.111.111)가 프락시 서버를 이용하여 피해자 시스템(123.123.123.123)에 접속하는 과정을 보이고 있다(모방 공격을 피하기 위해 상세한 명령 등은 생략함). 이때, 실제 피해자 시스템에서는 프락시 서버(222.222.222.222)에서 공격이 이루어진 것으로 나타나며, 실제 공격자를 추적할 수 없다. 또한, 외부에 공개된 프락시 서버를 통해서 내부 시스템으로 접근할 수 있을 가능성도 존재한다.



(그림 1) 프락시 서버를 이용한 접속

(그림 2)는 불법적으로 광고성 메일을 보내고자 하는 스패머가 프락시 서버를 이용하여 발송자 출처를 속여 다수의 사용자에게 메일을 발송하는 과정을 보이고 있다.
메일이 발송된 주소를 추적하기 위해 수신된 메일의 헤더에서 Received 부분을 분석하게 되는데 프락시 서버를 이용하여 발송하였을 경우 최초의 발송 주소가 프락시 서버 주소로 기록된다.

자신의 실제 주소를 속이기 위한 목적 이외에 프락시 서버를 이용하여 스팸메일을 발송하는 또 다른 이유가 있다. 외부에 메일 릴레이를 허용하여야만 하는 메일서버의 경우 스패머들이 사용할 수 없도록 RBL(Realtime Blackhole List) 등을 이용하여 스패머들이 메일 서버를 사용하지 못하도록 하는 경우가 많다. 스패머들은 직접적으로 자신의 주소를 사용하지 않고 프락시 서버의 주소를 사용함으로써 이를 우회하여 메일서버를 이용할 수 있게 된다.

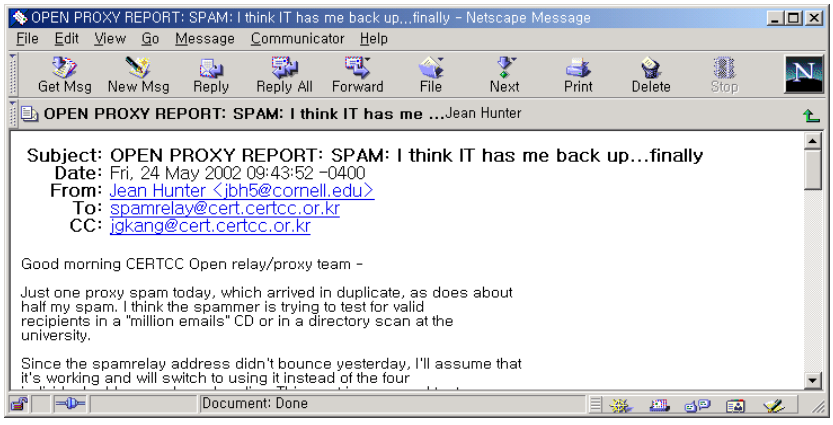


(그림 2) 프락시 서버를 이용한 스팸메일 발송

4. 공격 사례

최근 국내외로부터 스팸과 관련된 항의메일을 수없이 접수하고 있다. 이들 항의성 메일 중 상당수가 국내의 프락시 서버가 스팸 발송자들에게 사용되어 열려진 프락시 서버에 대한 조치를 부탁하는 메일이었다.

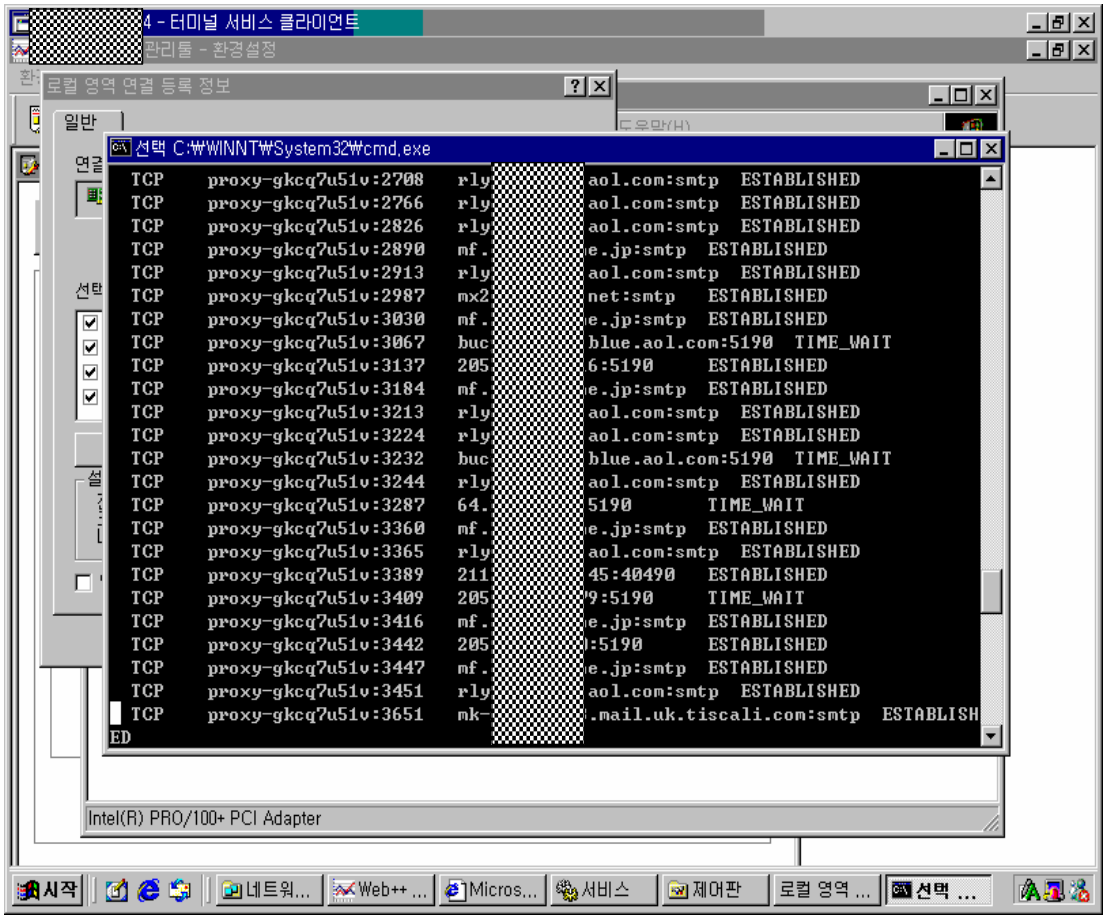
다음은 국외로부터 접수된 프락시 서버에 대한 항의 메일 중의 하나이다.



(그림 3) 국외에서 접수된 열려진 프락시 관련 항의메일

신고된 기관을 추적한 결과 국내 S 초등학교였으며, 유해 사이트 차단목적으로 프락시 서버(운영체제는 윈도우즈 2000서버였음)를 운영 중에 있었다.

해당시스템에 터미널 서비스를 통해 접속하여 분석하는 과정에서 (그림 4)와 같이 분석할 당시에도 S 초등학교의 프락시 서버를 통해 국외의 수많은 메일 릴레이 서버에 접속하여 스팸메일을 발송하고 있었다. S 초등학교 담당교사는 최근 프락시 서버가 현저하게 네트워크 속도가 저하되었다고 이야기했다.



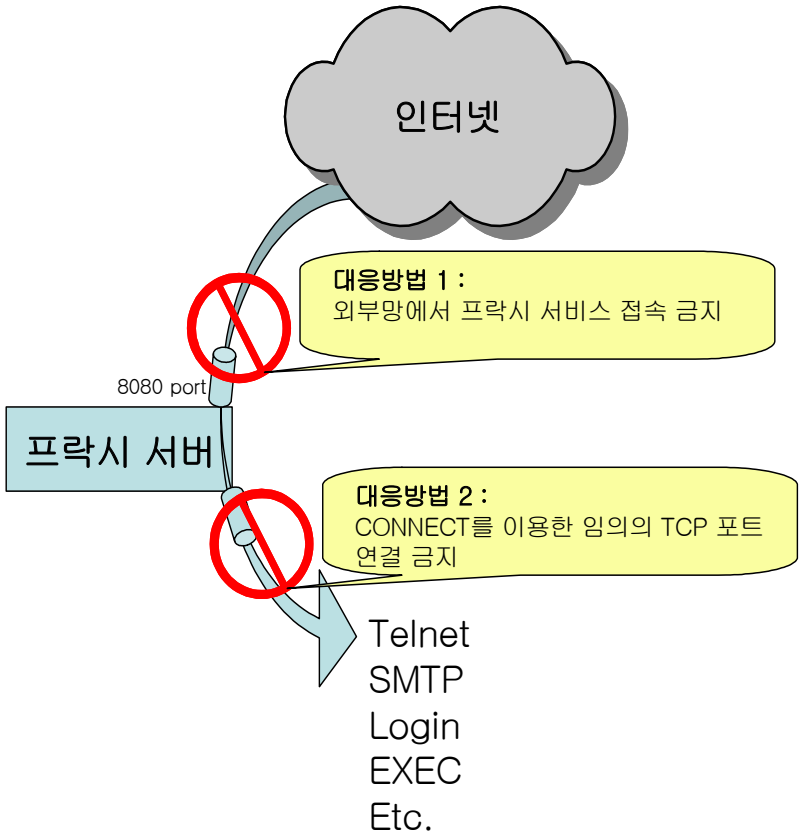
(그림 4) 국내 프락시 서버가 스팸메일 발송에 사용되고 있는 화면

비단 S 초등학교 뿐만 아니라 신고 접수된 많은 기관에서도 분석 당시에 스팸 메일 발송에 이용되고 있었다. 이로 인해 시스템 및 네트워크 속도가 현저히 저하되고, 시스템이 불안전하다는 호소들이 있었다.

5. 대응방법

먼저 사용중인 프락시 서버를 최신 버전으로 업그레이드하는 것이 가장 안전할 수 있다. 최근에 release되고 있는 많은 프락시 서버들은 이러한 문제들을 패치한 상태로 출시되고 있다.

그리고, 현재 사용중인 프락시 서버의 설정을 바꾼다. 프락시 서버의 설정파일을 점검하여 외부망에서 프락시 서비스로의 접근이 가능한지 또는 HTTP CONNECT 방법을 이용하여 임의의 TCP 포트로 연결을 허용하는지를 점검한다(그림 5).



(그림 5) 프락시 서버에서 보안설정

프락시 서비스들에 대한 접근은 신뢰된 네트워크에서만 가능하도록 하고 프락시 서버를 통해 임의의 TCP 포트가 아닌 특정 포트로만 연결되도록 설정하여야 할 것이다.

프락시 서버는 앞서 언급한 바와 같이 종류가 대단히 다양하고 제품에 따라 설정 방법도 서로 다르다. 각자 사용 중인 프락시 서버에서 (그림 5)와 같은 2가지 설정이 정상적으로 이루어져 있는지 확인해 보기 바란다.

국내에서 시판되고 있는 프락시 서버 중 탑플리시, 보라매, 포트라, 썬더웹에 대한 릴레이 차단 방법은 다음 문서를 참고하기 바란다.

스팸릴레이 방지관련 업체별 보안패치 :
http://www.certcc.or.kr/paper/tr2002/tr2002_04/spam8080.pdf

본 고에서는 이러한 설정을 설명하기 위하여 가장 광범위하게 사용되고 있는 공개용 프락시 서버 중의 하나인 Squid를 예로 들어보기로 한다.
또한 지금까지 언급한 HTTP CONNECT 방법은 아니지만, 기존에도 인터넷 주소를 세탁하기 위해 가장 많이 사용되고 있는 Wingate에서의 설정방법도 간단히 살펴보기로 한다.

가. Squid

Squid는 유닉스 특히, 리눅스를 기반의 프락시 서버로서 http://www.squid-cache.org에서 입수할 수 있으며, 현재까지 Squid 2.4버전까지가 안정화되어 공개되어 있다.

Squid-cache.org가 밝히는 Squid의 특징은 다음과 같다.

- 완벽한 웹 프락시 캐시 기능을 제공함
- 유닉스 시스템을 운영기반으로 함
- 누구나 자유롭게 사용할 수 있음(Free, Open Source Software)

또한 Squid는 아래와 같은 기능들을 제공한다.

- proxying and caching of HTTP, FTP, and other URL's
- proxying for SSL
- cache hierarchies

- ICP, HTCP, CARP, Cache Digests
- transparent caching
- WCCP (Squid v2.3 and above)
- extensive access controls
- HTTP server acceleration
- SNMP
- caching of DNS lookups

Squid 프락시 서버는 기본적으로 TCP 3128 포트를 사용한다. 따라서 TCP 3128 포트와 관련된 네트워크 트래픽을 찾는다면 Squid 프락시 서버일 가능성이 있다. 물론 해당하는 포트의 변경도 가능함에 유의해야 한다.

(그림 5)에서 언급한 2가지 대응방법을 Squid에서 설정하는 방법을 알아보도록 하자.

Squid에서 접근제어를 하기 위한 설정 파일은 /etc/squid/squid.conf 이다.

먼저, 첫 번째 대응방법인 외부망에서 프락시 서비스 접근금지를 위한 설정을 하도록 하자.

Squid는 기본적으로 모든 접속시도를 거부하게 설정되어 있다. 그러므로 신뢰할 수 있는 시스템들을 정의하고, 설정파일에 추가하는 것은 순전히 시스템관리자의 책임이다. 만일 Squid의 설정오류로 누구나 프락시 서버에 접근가능하다면 자신의 위치를 숨기고자하는 공격자에게는 더할 수 없이 좋은 경유지가 될 것이다.

그러면, 내부 네트워크를 222.222.222.x로 가정하고, 이 C-클레스에서만 프락시 서버로 접근가능하도록 설정하는 방법을 알아보도록 하자.

Squid에서는 ACL(Access Control List) 항목을 설정하여 프락시 서버에 대한 접근을 누구에게 허용할 것인가를 설정하는데 있어 범주를 정한다.

```
acl all src 0.0.0.0/0.0.0.0
acl localhost src 127.0.0.1/255.255.255.255
acl user-defined-name src 222.222.222.0/255.255.255.0
```

위는 all, localhost, user-defined-name의 이름으로 세 개의 ACL를 구성한 예이며, 사용자가 정의한 이름으로 IP 또는 IP 범위를 지정할 수 있다.

또한 ACL 이름 뒤에 키워드 src/dst를 명시하고 있는데, src(Source)는 접속을 요구하는 시스템을 의미하며, dst(Destination)은 접속대상이 되는 시스템을 의미한다.

그 다음으로, http_access 항목에 allow, deny 명령을 명시하면 웹서비스에 대한 접근을 IP 대역별로 통제할 수 있다.

```
http_access allow localhost
http_access allow user-defined-name
http_access deny all
```

위와같은 설정은 내부네트워크 즉, 222.222.222.x와 로컬 호스트에서만 프락시 서버로의 접근을 가능하게 한다.

두 번째 대응방법인 임의의 TCP 포트로 접속을 제한하는 방법에 대해서 알아보자.

아래의 예는 시스템관리자가 80, 443, 210, 119, 70, 21, 1025-65535 포트를 제외한 다른 포트들에 대해 접속을 제한하는 설정 예이다.

```
acl Safe_ports port 80 443 210 119 70 21 1025-65535
http_access deny !Safe_ports
```

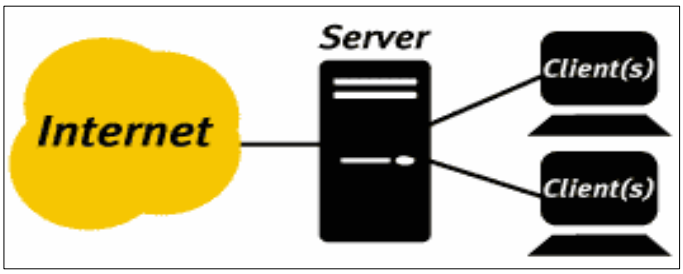
메일전송을 위한 SMTP와 웹서비스를 위한 HTTP는 서로 유사하게 설계되어 다. 이것은 곧 HTTP 프락시를 통해서 SPAM 릴레이를 할 수 있다는 의미를 내포하고 있다. 따라서, 프락시의 25(SMTP) port에 대한 HTTP 요구를 차단해야만 스팸 릴레이 요소를 제거할 수 있다. Squid는 이러한 문제를 해결하는 방향으로 기본설정되어 있다. 위의 포트 설정 예에서도 SMTP(25 포트)가 안전한 포트(Safe_ports)목록에 없음을 알 수 있다.

나. Wingate

Wingate는 디어필드(www.deerfield.com)사가 제작한 Windows 기반의 인터넷 공유 프로그램으로 라우터와 프락시 서버 기능을 동시에 제공하고 있다. 특히, Wingate는 ADSL, 위성인터넷, ISDN, 일반모뎀, 전용선 등의 인터넷서비스의 종류에 구애받지 않으며, 단 한대의 Wingate 서버를 인터넷에 연결함으로서, 인터넷 연결을 공유할 수 있으므로 적은 비용으로 네트워크를 구축할 수 있다.

Wingate의 가장 중요한 기능 2가지는 아래와 같다.

- 내부 네트웍과 인터넷 사이에서 인터넷 트래픽 라우팅
- 내부 네트웍의 컴퓨터의 요청에 따른 네트웍 주소(IP Address)를 자동부여



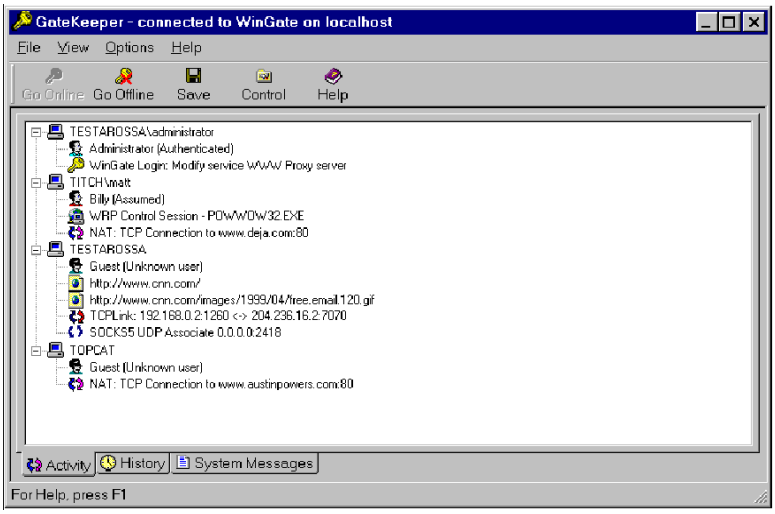
(그림 6) Wingate 서버를 이용한 네트워크의 구축

Wingate는 자체적인 Firewall 기능을 제공하여 게이트웨이 컴퓨터(즉, Wingate가 설치된 인터넷 접속점)와 Wingate 안쪽의 내부 네트워크를 보호한다. Firewall을 통해서 Wingate가 제공하는 부와서비스를 개략적으로 살펴보면 아래와 같다.

패킷 필터링 : 프로토콜, 인터페이스, 포트 등을 기준으로 접속 허가/불가/다른 시스템으로 의 forwarding 여부를 결정

- 침입 기록 : Wingate 시스템으로의 접근 시도중 의심가는 활동을 로깅함

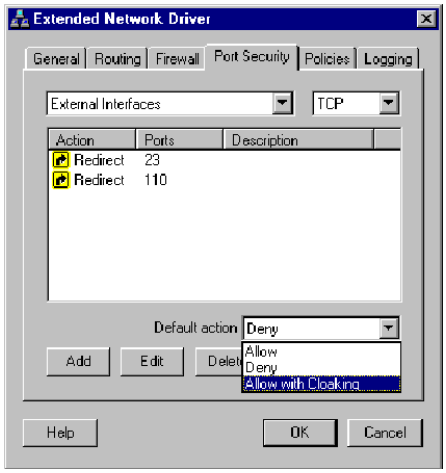
이러한 Firewall기능은 Wingate의 설정, 관리, 운영을 총괄할 수 있는 사용자 인터페이스인 게이트키퍼(GateKeeper)를 통해서 행할 수 있다. 아래 그림은 게이트키퍼의 초기 실행화면이다.



(그림 7) 게이트키퍼에 접속한 화면

구체적인 모든 세부사항을 전부 언급할 수는 없으므로, 포트에 대한 접근제어만을 예로 설명하겠다. 게이트기퍼의 Extended Network Driver항목을 선택하여 “Firewall 탭”과 “Port Security 탭"의 내용을 설정하면 원하는 포트별로 접근을 제어할 수 있다.

(그림 8) Firewall 기능의 설정



(그림 9) 포트에 대한 접근설정

※ 이러한 Firewall설정은 Wingate 스탠다드/프로 버전을 기준으로 한 것임.

보다 상세한 제품설명은 http://wingate.webservice.co.kr에서 한글로 제공되는 매뉴얼에서 찾을 수 있으며, 2002년 6월 20일 현재 디어필드사는 WinGate 버전 5.0 Beta를 자사 홈페이지에 공개하고 있다.

6. 결론

최근 국내 프락시 서버를 이용한 대량의 스팸 메일 발송으로 인해 국외로부터 수많은 항의 메일이 접수되고 있으며 국가 신인도도 실추되고 있다.
프락시 서버는 스패머들 뿐만 아니라 범죄를 목적으로 인터넷을 사용하려고 하는 모든 사람들에게도 좋은 목표물이 되고 있다.

프락시 서비스는 웹 프락시, 캐쉬 서버, Firewall 등 대단히 다양한 목적으로 사용되고 있으며, 일선 회사에서도 광범위하게 사용되고 있다.

우리 기관에서 운영 중인 프락시 서버를 통해 범죄가 이루어지고 있지 않는지 점검해 볼 필요가 있다.