작성자 : 기술지원부 김 삼 수 <kiss@nextline.net>

TCP-Wrapper 구성

(1) TCP-Wrapper란?

슈퍼 데몬(xinetd)에 영향을 받는 데몬들은 Tcp-Wrapper 프로그램에 의해 접근이 제어되며 Tcp-Wrapper를 이용하면 특정 서비스에 대해 접근자의 호스트를 체크해서 접근을 허락할지 결정을 할 수 있습니다. Tcp-Wrapper에 영향을 받는 대표적인 데몬으로는 telnet과 ssh, ftp, pop3등이 있습니다. Tcp-Wrapper는 /etc/hosts.allow파일을 통해서 접근 허가를 하고 /etc/hosts.deny파일을 통해서 접근 거부를 결정합니다.

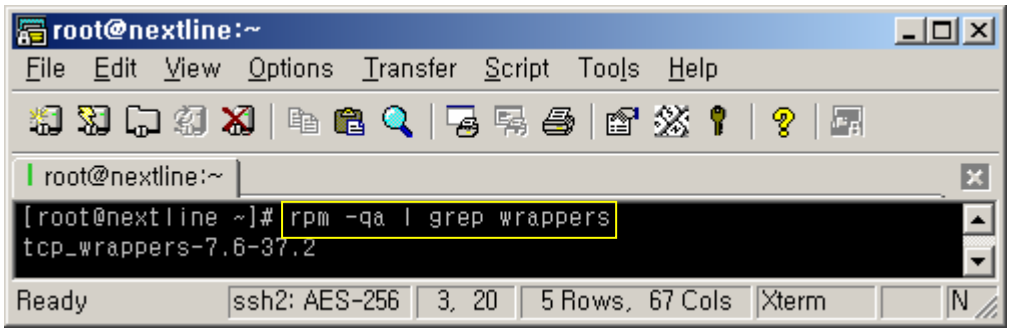
inetd를 사용하던 레드헷 7.0 이전 버젼에서는 tcpd를 이용해서 Tcp-Wrapper의 영향을 받게 설정을 했는데 레드헷 7.0 이상 버젼에서는 xinetd 컴파일시에 libwrap을 지원하게 설정되어 있어서 tcpd보다 더 효률적으로 Tcp-Wrapper를 사용할 수 있습니다.

그래서 /etc/xinetd.d/ 디렉토리안의 서비스 파일에 tcpd 설정을 해 줄 필요가 없습니다. 단지 hosts.allow 파일과 hosts.deny 파일만 설정해 주면 Tcp-Wrapper 기능을 사용할 수 있습니다. Redhat7.0 부터는 TCP_Wrapper와 유사하나 보다 강화된 Xinet가 기본적으로 설치되어 있습니다.

rpm 조회옵션
-q : 패키지가 설치되어 있는지 질의하며 이 옵션을 단독으로 사용하면 패키지 이름과 버젼만 표시됩니다.
-qa : 현재 설치된 모든 패키지 목록을 찾는데 사용합니다.
-qi : 현재 설치된 패키지의 간략한 정보를 출력합니다.
-ql : 현재 설치된 패키지의 내용을 보여주며 어떤 파일이 어디에 설치되어 있는지 확인할 때 사용합니다.
-qa, -qi, -ql 옵션은 보통 grep명령과 같이 사용됩니다.
특정 rpm패키지의 설치여부 확인하기
사용형식 : rpm -qa | grep 확인하고자 하는 패키지 이름문자열
“|” 파이프 : 앞의 rpm -qa한 결과를 그대로 grep에게 넘겨주는 겁니다. grep는 어떤 패턴에 맞는 것을 뽑아내는 역할을 주로 하는데 앞에서 넘어온 rpm패키지 리스트 중에서 패키지 이름문자열에 해당하는 것만 뽑아내게 됩니다.

① Tcp-Wrapper가 설치되어 있는지 확인합니다.
[root@nextline ~]# rpm -qa | grep wrappers

Tcp-Wrapper가 설치되어있지 않을 경우 Tcp-Wrapper설치 문서를 통해 설치를 합니다.



(2) Tcp-Wrapper 설치

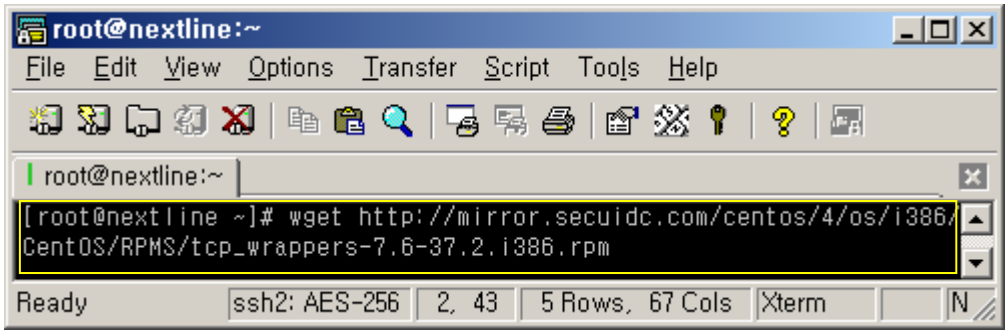
rpm패키지를 다운로드 합니다.

CentOS

http://mirror.secuidc.com/centos

Fedora Core

http://download.fedoralegacy.org



② Tcp-Wrapper 설치

rpm패키지 설치옵션

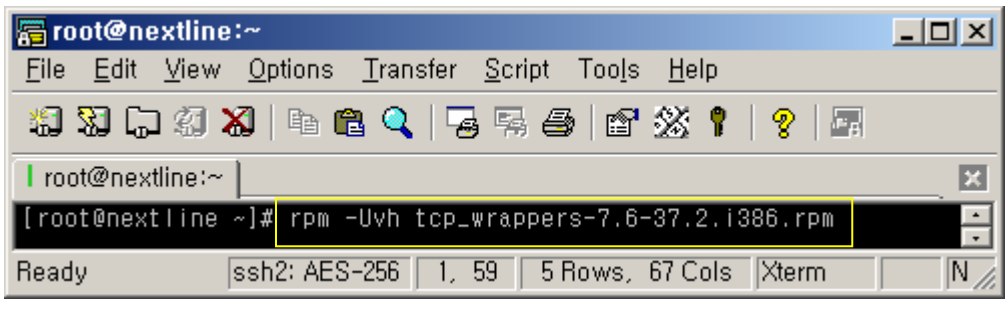
rpm -U 옵션 : 이전버젼이 설치되어 있으면 업그레이드를 하며, 설치되어 있지 않으면 새롭게 설치합니다. 이전버젼이 설치되어 있을 경우에 환경설정파일을 제외하고 모두 새롭게 설치하게 되며 설치시에 이옵션을 사용하도록 합니다.

rpm -v 옵션 : 설치 중 메시지를 보여줍니다.

rpm -h 옵션 : 진행과정을 '#'으로 표시합니다. (--hash)

다운로드 받은 Tcp-Wrapper rpm패키지를 설치합니다.

[root@nextline ~]# rpm -Uvh tcp_wrappers-7.6-37.2.i386.rpm



(2)TCP-Wrapper 설정

① 접속과정

[Server Demon이 Tcp-Wrapper에 의해 보호받고 있을 때 접속 과정]

Server Demon : telnet, ssh, ftp, pop3등을 구동시켜주는 데몬을 말합니다.

Client 접속 요청 --> xinetd --> Tcp-Wrapper --> Demon 실행

위의 과정에서 xinetd는 해당 Demon으로 접속 요청이 있을 경우 바로 해당 Demon을 실행하는 것이 아니라 Tcp-Wrapper를 거치게 되어 있습니다. 이렇듯 각 Demon들은 Tcp-Wrapper의 보호막에 감싸져 있다고 생각하면 됩니다. Tcp-Wrapper을 통과할 수 있는 조건은 hosts.deny에서 거부하지 않거나 hosts.allow에서 접근을 허락해야 됩니다.

② 데몬과 클라이언트 설정

hosts.deny, hosts.allow은 /etc디렉토리에 존재합니다.

그럼 지금부터 hosts. 파일을 어떻게 설정하는지 살펴 보도록 합니다.

hosts.allow, hosts.deny 설정형식

Demon_List: Client_List: options(생략가능): options(생략가능)...

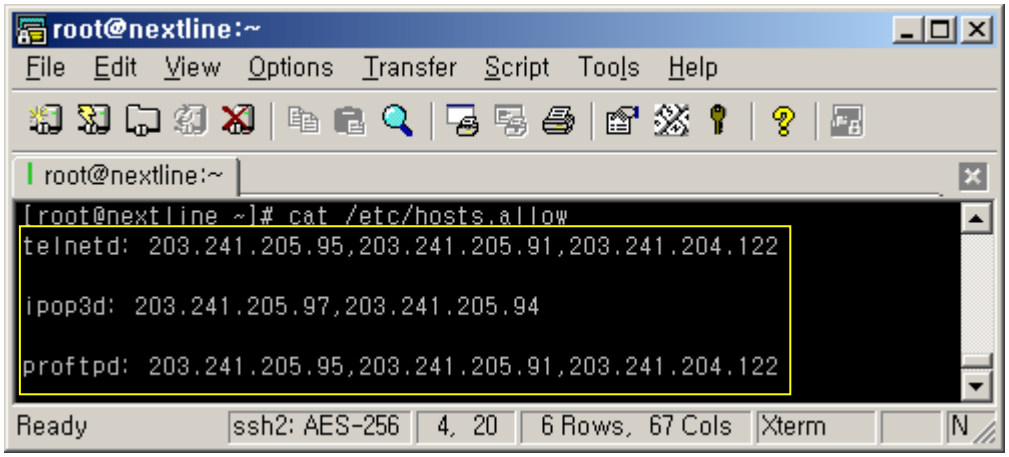
Demon_List, Client_List, options는 :(콜론)으로 구분됩니다.

Demon_List 설정

Tcp-Wrapper로 접근을 제어할 서비스를 설정해야 합니다.

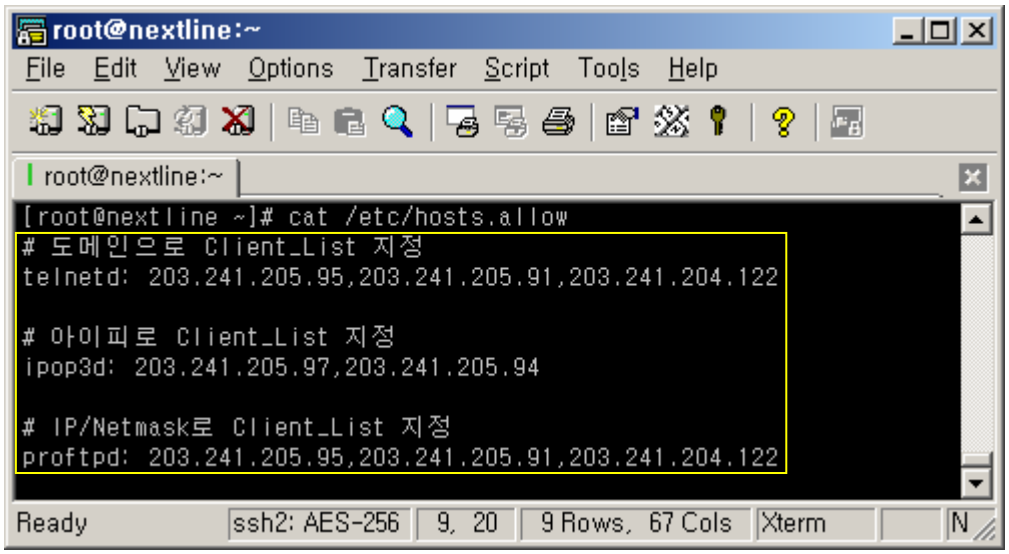
주의할 것은 xinetd에 설정된 서비스 네임이 아니라 실제 그 서비스를 가동시키는 데몬 프로그램을 적어 줘야 됩니다. (예: telnet이 아니라 telnetd를 설정해야 됩니다.)

즉 각 서비스의 xinetd 설정 파일에서 "server" 지시자로 설정해준 프로그램을 적어 주면 됩니다. "ALL" 이라는 와일드 카드는 Tcp-Wrapper에 영향을 받는 모든 데몬들을 가리킵니다.



Client_List 설정

Tcp-Wrapper로 접근을 제어할 클라이언트를 정의하는 부분입니다. 클라이언트 정의는 도메인, IP주소, IP/Mask등으로 설정할 수 있고 와일드 카드와 패턴을 적용 시킬 수도 있습니다. 두개 이상의 호스트를 설정할 경우에는 ,(콤마) 또는 빈 공간으로 각 호스트를 구분해주면 됩니다. "ALL"은 모든 호스트를 나타내는 와일드 카드입니다.



도메인을 이용한 Client_List 설정

도메인으로 설정할 경우에는 반드시 reverse mapping이 되는 도메인만 설정 가능합니다.
(예: nslookup xxx.xxx.xxx.xxx --> nextline.co.kr)
패턴을 이용해서 모든 서브 호스트에 대해서 설정할 수 있으며 서브 호스트에 대한 패턴 설정은 .(점)으로 합니다.
(예: .nextline.co.kr ---> nextline.co.kr 의 모든 하위 도메인에 대해서 설정한 것입니다.)

IP 주소를 이용한 Client_List 설정

제어할 클라언트의 IP주소를 설정합니다. IP주소도 .(점)으로 패턴을 적용할 수 있으며
(예: 203.241. --> IP주소가 203.241.x.x 인 모든 호스트를 나타냅니다.)

IP/NetMask를 이용한 Client_List 설정

IP주소와 넷마스크를 이용해서 대상 클라이언트를 설정할 수 있는데 패턴으로 똑같이 처리할 수 있기 때문에 C클래스를 다시 서브넷으로 나누어 쓰는 호스트들을 제어 할 때만 주로 사용됩니다.

(예: 203.241.205.0/255.255.255.128 --> 아이피 주소 203.241.205 ~ 126)

EXCEPT

패턴 또는 IP/Netmask를 이용해서 다수의 호스트를 설정할 때 특정 호스트를 제외 시킬 수 있습니다.
(예: 203.241.205.0/255.255.255.0 EXCEPT 203.241.205.95 --> 203.241.205.95를 제외한 C 클래스 203.241.205.x)

(3)TCP-Wrapper 옵션

options 설정
꼭 설정해야 되는 부분은 아닙니다. options 설정을 이용해서 허가 되지 않는 호스트에 대해서 경고 메시지를 보내는 등 호스트 연결을 거부하거나 허락하기 전에 특정 명령을 실행 시킬 수 있습니다. 쉘 명령을 실행 시키지 위한 방법으로는 twist또는 spawn을 사용합니다. 쉘 명령을 설정할 때는 반드시 절대 경로로 정확히 설정해 주어야 됩니다. 또 'banners'라는 설정으로 client에게 텍스트 문서를 보여줄 수도 있습니다.

vi 에디터 사용법
사용형식 : vi [옵션] [생성할 파일명/편집할 파일명]

vi 에디터는 입력모드, 명령모드, 실행모드로 구분됩니다.

입력모드 : vi 편집화면에서 문자를 입력할 수 있는 모드로서 입력모드로 진입하기 위해서는 i, a, o, I, A, O, R등이 있습니다. 즉 초기 vi 편집기 모드는 명령어 모드로 진입을 하기때문에 문자를 입력하기 전에 앞의 단축키중 하나를 먼저 입력해야 원하는 문자를 입력할 수 있습니다.
명령모드 : 커서이동/문자삭제/문자(열)교체/문자열검색 등을 할수 있는 모드로서 입력모드에서 편집이 완료되면 Esc키를 눌러 명령모드로 진입하면 됩니다.

실행모드 : 특별한 명령어를 실행하는 모드로서 명령어모드에서 ":"(콜론)를 누르면 vi 화면 하단 좌측에 vi 특수명령어를 입력할 수 있습니다.

실행모드의 일반적으로 쓰이는 특수 명령어
q : 수정 작업이 이루어지지 않은 상태에서 vi 편집기에서 빠져나옵니다.
q! : 수정 작업이 이루어진 부분을 적용시키지 않고 vi 편집기를 강제로 빠져나옵니다.

w : 수정된 작업을 저장합니다.

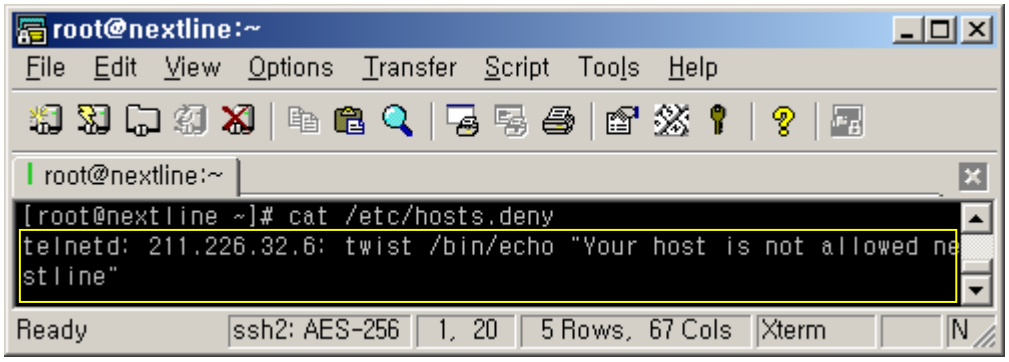
wq : 수정된 작업을 저장하고 vi 편집기에서 빠져나옵니다.

초기 명령어모드 -> 입력모드진입 -> 편집 -> 명령어모드 -> 실행모드 -> 종료

① twist

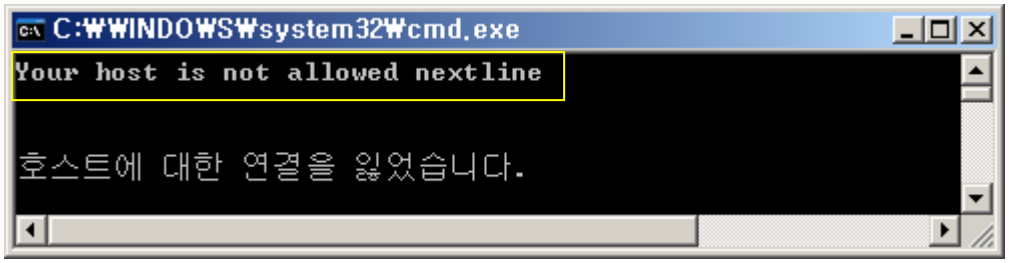
twist는 명령의 결과를 client에게 전송하기 때문에 client에게 메시지를 보낼 때 유용합니다.

211.226.32.6 아이피 접속시 "Your host is not allowed nextline" 보냅니다.



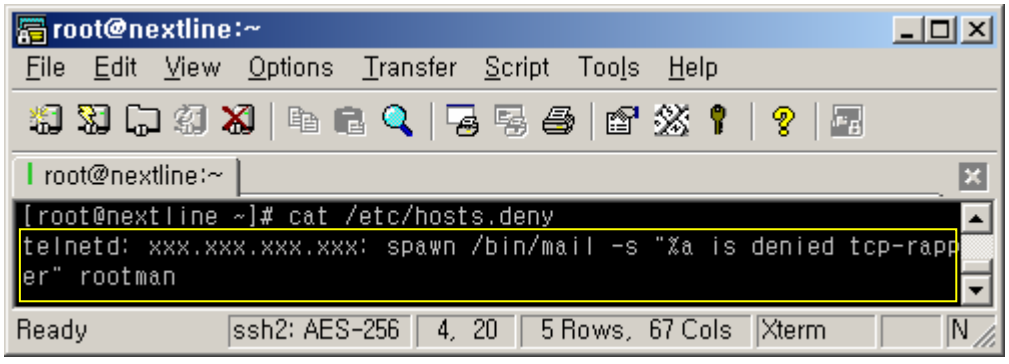
윈도우 cmd창에서 xxx.xxxxxx.xxx로 접속을 시도하는 화면입니다.

211.226.32.6에서 텔넷 접근을 시도할 때 클라이언트에 출력되는 메시지 입니다.



② spawn

twist와 같이 쉘 명령을 실행 시켜 주는데 명령의 결과를 client에게 전송하지 않습니다.

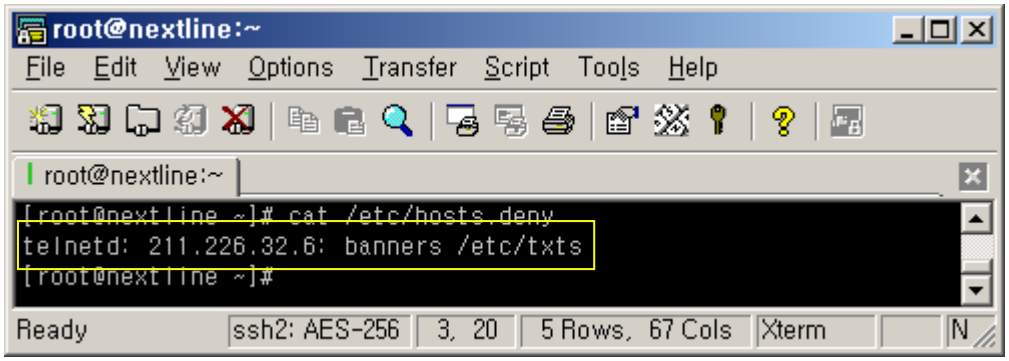


위의 설정은 호스트 xxx.xxx.xxx.xxx에서 텔넷 접근을 할 경우 접근을 거부하면서 사용자 rootman에게 "%a is denied tcp-wrapper" 라는 제목으로 메일을 발송합니다. %a는 Tcp-Wrapper의 환경 변수로 client의 IP주소를 나타냅니다.

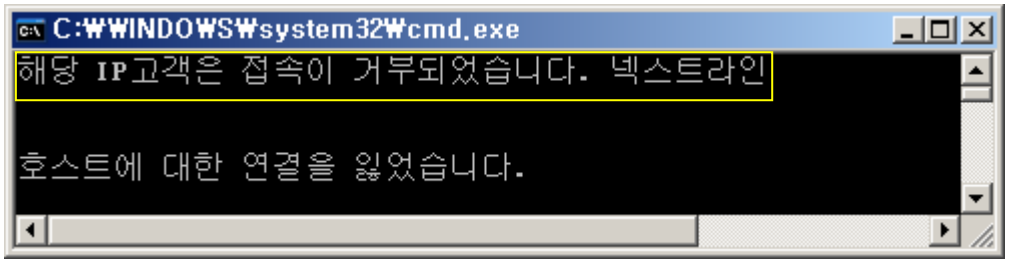
shell_command에서 사용가능한 환경 변수
%a : 클라이언트 IP 주소
%c : 클라이언트 정보(User@Host, User@Address, 호스트 네임, 또는 IP 주소)
%d : 데몬 프로세스 이름(예: telnetd, ftp, pop3)
%h : 클라이언트 호스트 네임 또는 IP주소
%n : 클라이언트 호스트 네임(or"unknown" or"paranoid")
%p : 데몬 프로세스 아이디(PID)
%s : 서버 정보(demon@host, demon@address, 데몬 이름)
%u : 클라이언트 사용자 이름(or "unknown")
%% : 하나의 '%'문자

③ banners
banners로 특정 디렉토리를 지정하면 디렉토리 내의 문서를 client로 출력 시켜 줍니다. 문서 파일명은 Demon_List와 동일해야 됩니다. 예를 들면 접속 호스트가 telnetd에 대해서 설정한 Client_List와 일치할 경우 지정한 디렉토리 내의 telnetd 라는 파일을 client로 출력합니다.

/etc 디렉토리에 txts디렉토리 생성 후 vi 에디터를 이용하여 telnetd 파일을 생성하여 “해당 IP고객은 접속이 거부되었습니다. 넥스트라인” 문구를 출력되도록 합니다.



211.226.32.6에서 텔넷 접근을 시도할 때 클라이언트에 출력되는 메시지 입니다.



/etc/txts 라는 디렉토리를 만들고 그 안에 telnetd라는 텍스트 파일을 만들어야 합니다.

(4) 적용사례

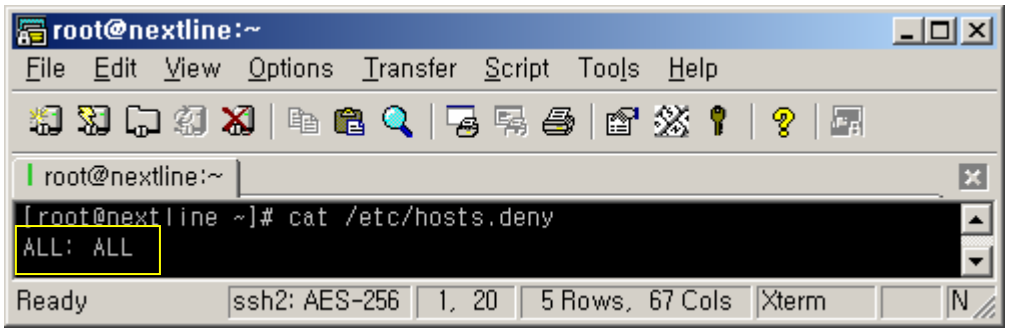
TCP-Wrapper의 경우 hosts.deny에서 모든 데몬과 ip에 대해 거부를 한 뒤 hosts.allow에서 허용 하도록 하는 TCP-Wrapper설정이 보편적으로 사용됩니다. tcpd는 먼저 hosts.allow에 의해서 검사해서 서비스가 허가되었으면 허가합니다. 그리고 나서 hosts.deny에 의해서 서비스가 금지되었으면 금지합니다. 그리고 나머지 서비스는 허가합니다.

메일서버, ftp를 사용하며 관리자 접속 IP 123.123.123.12인 경우의 TCP-Wrapper를 설정해 보도록 하겠습니다.

① hosts.deny 설정

/etc/hosts.deny에서 모든 호스트와 데몬에대해 “ALL: ALL” 옵션을 적용합니다.

ALL: ALL



② hosts.allow 설정

로컬허용을 합니다. (로컬이 거부되어 있을 시 로컬메일 발송 및 php mail()함수 사용시 메일이 발송되지 않게 됩니다.

ALL: LOCAL

ALL: 127.0.0.1

내부아이피를 이용하여 DB서버를 구축하신 경우 접속 가능토록 192.168.0.2 허용합니다.

ALL: 192.168.0.2

관리자가 접속 할 수 있도록 관리자 PC의 아이피를 허용합니다.

ALL: 123.123.123.12

메일서버(sendmail, ipop3, dovecot)를 모두 허용합니다.

sendmail: ALL
ipop3d: ALL
dovecot: ALL
ftp의 모든 접속을 허용합니다.
vsftpd: ALL
proftpd: ALL