TCP WRAPPER
It is used to restrict the systems to access the services. Here we have the access checking in three stages.
1. Access Explisitly Permited
2. Access Explisitly Denied
3. By Default Permit Access

Configuration of TCP Wrappers Stored in Two Files :
1. /etc/hosts.allow :
This file is used to give the permissions to access the services.
2 etc/hosts.deny:
This file is used to deny the permissions to access the services.
syn : deamon-list : client-list {:options}

deamon-list:
Here deamon specifications are mentioned. If we want to specify more than one dearnon have to delimit those deamons with a ","(cama symbol).

client-list :
This field specifies the clients. If more than one client how to specify then they have to delimited by ","(cama).
here we can use ip address (or) domain name (or) hostname with subnet mask.

Here we will be using two keywords :
1. ALL : This key word is used to specify all the deamons (or) clients.
2. EXEPT : To specify only to a perticular deamon.
The functionality of this two keywords are changed from the two files /etc/hosts.allow, /etc/hosts.deny

examples :
To deny the system 192.168.0.2 to access 192.168.0.1 through ssh (secure shell)
Open the file /etc/hosts.deny and add bellow line
sshd : 192.168.0.1
To restrict all the hosts in india.com
#vi /etc/hosts.deny
sshd : *.india.com
To restrict all the hosts in india.com exept sun3.india.com
vi/etc/hosts.deny
sshd *.indiacom EXEPT sun3.india.com

To restrict all wrappered services to every one
vi /etc/hosts.deny
ALL:ALL
The above example denies access to all TCP Wrappers services to every one except those who are explisitily allowed
vi /etc/hosts.allow
ALL:127.0.0.1 #all the services to the local system
vsftpd : 192.168.0 #it indicates all the systems in the network 192.168.0
in.telnetd,sshd : .example.corn #allows hosts in the example.com to access.telnet, ssh services.