#

> TCP Wrapper是一个基于主机的网络访问控制表系统，用于过滤对类Unix系统（如Linux或BSD）的网络访问。对基于tcp开发并提供服务的应用程序，提供的一层访问控制工具。尽管TCP Wrappers不能替代防火墙，但可以结合防火墙使用TCP Wrappers可以给系统增加一道安全防线。
>
> TCP Wrapper基于库调用实现其功能，只有由super daemon管理的服务以及有支持libwarp.so动态库的程序才可以支持TCP Wrappers。任何由xinetd管理的服务都支持TCP Wrappers机制。

判断某服务是否能够由TCP Wrapper进行访问控制

```
ldd $(which DAEMON_NAME) | grep libwrap
```

实现方法

> 在配置文件中为各服务分别定义访问控制规则实现控制访问：
>
> /etc/hosts.allow
>
> /etc/hosts.deny

> *定义文件检查次序：先检查hosts.allow文件，如果有定义，则放行;如果没有定义,再检查hosts.deny文件，如果有定义，则拒绝;如果有定义，则默认允许。可以在hosts.deny中定义拒绝所有服务，然后在hosts.allow中以白名单的形式开放服务。*

配置文件语法

```
daemon_list : client_list [EXCEPT] [: option] [ :
shell_command ]
```

> `daemon_list`:应用程序的文件名称，不是服务名称;可以有多个应用程序名称，用逗号隔开。ALL所有服务

> `client_lsit`: IP地址;主机名;网络地址,必须使用完成格式的掩码，例如192.168.1.150/255.255.255.0;ALL,所有主机;KNOWN:所有可以解析的主机;UNKNOWN:所有无法解析的主机。

> `EXCEPT`：后跟某个网段内特定允许或拒绝的IP

> `option`：deny：在hosts.allow文件中实现拒绝的功能；allow：在hosts.deny文件中实现允许的功能；spawn：启动额外的应用程序

更多语法释义参考man文档。hosts.allow、hosts.deny。