Linux 防火墙配置

所谓防火墙指的是一个由软件和硬件设备组合而成、在内部网和外部网之间、专用网与公共网之间的界面上构造的保护屏障.是一种获取安全性方法的形象说法，它是一种计算机硬件和软件的结合，使 Internet 与 Intranet 之间建立起一个安全网关（Security Gateway），从而保护内部网免受非法用户的侵入，防火墙主要由服务访问规则、验证工具、包过滤和应用网关 4 个部分组成，防火墙就是一个位于计算机和它所连接的网络之间的软件或硬件。该计算机流入流出的所有网络通信和数据包均要经过此防火墙。

防火墙，简单的说，就是针对源 IP 或域进行允许或拒绝的设置，以决定该连接是否能够成功实现连接的一种方式。

/etc/hosts.allow, /etc/hosts.deny 管理

基本上只要一个服务受到 xinetd 管理(通常情况可以查看/etc/xinetd.d/的内容来判断)，或者是该服务的程序支持 TCP wrapper 函数的功能时，那么该服务的防火墙的设置就可以通过以/etc/hosts.{allow,deny}来处理

配置文件语法：两个文件设置语法都一样，基本上，看起了应该像下面这个样子，其中'<' '>'是不存在于配置文件中的

<service (program_name)> : <IP,domain, hostname> : <action>

#注意，第一个字段里面的是启动服务的程序，而不是服务本身，例如 ssh 服务的启动程序应该为 sshd

例子：阻止下面两个 IP 使用 rsync 程序

[root@rhel6164 ~]# vim /etc/hosts.deny

rsync:127.0.0.100 127.0.0.200:deny

注意事项：

在两个文件中默认的 action 都是可以省略的，/etc/hosts.allow 默认的 action 为 allow，/etc/hosts.deny 默认 action 为 deny

两个文件的判断依据是，以/etc/hosts.allow 为优先，若分析到 IP 或网段不在/etc/hosts.allow，则以/etc/hosts.deny 来判断

一些在第一、第二字段里面的特殊字符

ALL：代表全部的 program_name 或者 IP 都接受的意思，例如 ALL:ALL:deny

LOCAL：代表来自本机的意思，例如 ALL:LOCAL:allow

UNKNOWN：代表不知道的 IP 或者是 domain 或者是服务时

KNOWN：代表为可以解析的 IP, domain 等信息时

iptables

和上面讲解的/etc/hosts.*一样，iptables 也是 Linux 自带的软件防火墙，iptables 是利用封装包过滤的机制，所以他会分析封装包的表头数据，根据表头数据与定义的规则来决定该封包是否可以进入主机或者被丢弃，意思就是，根据封包的分析资料“对比”你预先定义的规则内容，若封包数据与规则内容相同则进行动作，否则就继续下一条规则的比对，重点是对比是有顺序的

iptables 有三个重要的表

1. filter：主要跟 Linux 本机有关，这个是预设的 table

2. nat：这个表格主要在用作来源与目的之 IP 或 port 的转换，与 Linux 本机无关，主要与

Linux 主机后的局域网内的计算机有关
3. mangle：这个表格主要是与特殊的封包的路由旗标有关