|  |
| --- |
| **Iptables已经集成在[Linux](https://www.linuxprobe.com/" \o "linux" \t "_blank) 2.4及以上版本的内核中，同Windows下的众多“傻瓜”防火墙不同的是，Iptables需要用户自己定制相关规则。下面我就给大家简单介绍一下关于防火墙的基本操作。** |

**防火墙的初始化**

废话不多说，先上一张表格：

|  |  |
| --- | --- |
| 选项 | 含义 |
| -F | 清除链中所有的规则 |
| -P | 为链添加一条默认策略（目标） |
| -A | 为链增加一条规则说明 |
| -D | 从链中删除一条规则 |
| -L | 查看当前表的链和规则 |

清空默认表（filter表）中的数据，只要简单的使用下面这条[命令](https://www.linuxcool.com/" \o "命令" \t "_blank)即可：

[root@localhost ~]# iptables -F

清除默认表中INPUT链的规则，可使用下面的[命令](https://www.linuxcool.com/" \o "命令" \t "_blank)：

[root@localhost ~]# iptables -F INPUT

命令执行完成后，使用iptables -L查看当前防火墙设置。  
给链设置默认策略基本语法如下：

iptables -P archy target

其中archy是链的名称，target（目标）用于定义策略。  
filter表中共有9个不同的策略可供使用，但最常用的只有4个，分别包括：ACCEPT表示允许包通过；DROP丢弃一个包；REJECT会在丢弃的同时返回一条ICMP错误消息；LOG则扮演了记事员的角色记录包的信息。  
通常对服务器而言，将所有链设置为DROP是一个不错的选择，下面这条命令将所有的链的默认策略设置为DROP：

[root@localhost ~]# iptables -P INPUT DROP

执行完这条命令后，所有试图同本机建立连接的努力都会失败，因为所有从“外部”到达防火墙的包都会被丢弃，甚至连使用回环接口ping自己都不行。

**添加规则**

使用iptables  -A命令添加链规则，命令基本语法如下：

iptables -A archy -i interface -j target

其中，archy代表链的名称，interface指定该规则用于哪个网络接口，target用于定义策略。举一个很简单的例子，下面这条命令就是添加一条INPUT链的规则，允许所有通过lo接口的链接请求：

[root@localhost ~]# iptables -A INPUT -i lo -p ALL -j ACCEPT

其余有关防火墙规则的设置相关选项，如下表：

|  |  |
| --- | --- |
| 选项 | 含义 |
| -p proto | 匹配网络协议：tcp、udp、icmp |
| --icmp-type type | 匹配ICMP类型，和-p icmp配合使用。注意有两根短划线 |
| -s source-ip | 匹配来源主机（或网络）的IP地址 |
| --sport port# | 匹配来源主机的端口，和-s source-ip配合使用。 |
| -d dest-ip | 匹配目标主机的IP地址 |
| --dport port# | 匹配目标主机（或网络）的端口，和-d dest-ip配合使用。 |

**删除链规则**

iptables提供了-D选项来删除链规则，有两种不同的语法用于删除一条规则，这儿介绍最常用的方法：

首先使用带--line-numbers选项的iptables -L命令查看链规则的编号，命令如下：

[root@localhost ~]# iptables -L --line-numbers

当你查到规则编号后使用下面命令就可以删除连规则：

[root@localhost ~]# iptables -D 18