# pfctl

PF防火墙的配置命令

## 补充说明

**pfctl命令** 是PF防火墙的配置命令。PF防火墙( 全称：Packet Filter )是UNIX LIKE系统上进行TCP/ip流量过滤和网络地址转换的软件系统。PF同样也能提供TCP/IP流量的整形和控制，并且提供带宽控制和数据包优先集控制。PF最早是由DanielHartmeier开发的，现在的开发和维护由Daniel和openBSD小组的其他成员负责。

PF防火墙的功能很多，本站只列举一些基本配置。

### 激活

要激活pf并且使它在启动时调用配置文件，编辑`/etc/rc.conf`文件，修改配置pf的一行：

```
pf=yes
```

重启操作系统让配置生效。

也可以通过pfctl程序启动和停止pf。

```
pfctl -e
pfctl -d
```

注意这仅仅是启动和关闭PF。实际它不会载入规则集，规则集要么在系统启动时载入，要在PF启动后通过命令单独载入。

### 配置

系统引导到在rc脚本文件运行PF时PF从`/etc/pf.conf`文件载入配置规则。注意当`/etc/pf.conf`文件是默认配置文件，在系统调用rc脚本文件时，它仅仅是作为文本文件由pfctl装入并解释和插入pf的。对于一些应用来说，其他的规则集可以在系统引导后由其他文件载入。对于一些设计的非常好的unix程序。PF提供了足够的灵活性。

#### pf.conf文件有7个部分：

1. 宏：用户定义的变量，包括IP地址，接口名称等等。
2. 表：一种用来保存IP地址列表的结构。
3. 选项：控制PF如何工作的变量。
4. 整形：重新处理数据包，进行正常化和碎片整理。
5. 排队：提供带宽控制和数据包优先级控制。
6. 转换：控制网络地址转换和数据包重定向。
7. 过滤规则：在数据包通过接口时允许进行选择性的过滤和阻止。

除去宏和表，其他的段在配置文件中也应该按照这个顺序出现，尽管对于一些特定的应用并不是所有的段都是必须的。

空行会被忽略，以#开头的行被认为是注释。

## 控制

引导之后PF可以通过pfctl程序进行操作，以下是一些例子：

```
pfctl -f /etc/pf.conf  # 载入 pf.conf 文件
pfctl -nf /etc/pf.conf # 解析文件，但不载入
pfctl -Nf /etc/pf.conf # 只载入文件中的NAT规则
pfctl -Rf /etc/pf.conf # 只载入文件中的过滤规则
pfctl -sn # 显示当前的NAT规则
pfctl -sr # 显示当前的过滤规则
pfctl -ss # 显示当前的状态表
pfctl -si # 显示过滤状态和计数
pfctl -sa # 显示任何可显示的
```

完整的命令列表，请参阅pfctl的man手册页。