# Iptables教程

# iptables防火墙简介

Iptables也叫netfilter是Linux下自带的一款免费且优秀的基于包过滤的防火墙工具，它的功能十分强大，使用非常灵活，可以对流入、流出、流经服务器的数据包进行精细的控制。iptables是Linux2.4及2.6内核中集成的模块。

# Iptables服务相关命令

1. 查看iptables状态

service iptables status

1. 开启/关闭iptables

service iptables start

service iptables stop

1. 查看iptables是否开机启动

chkconfig iptables --list

1. 设置iptables开机启动/不启动

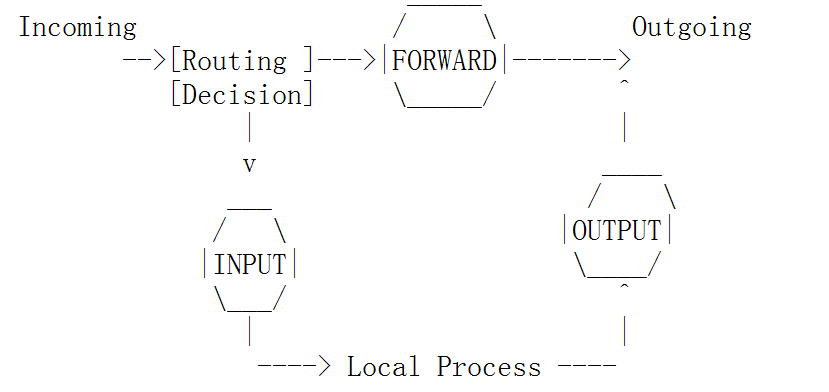
chkconfig iptables on

chkconfig iptables off

# iptables原理简介

## iptables的结构

在iptables中有四张表，分别是filter、nat、mangle和raw每一个表中都包含了各自不同的链，最常用的是filter表。



* **filter表：**

filter是iptables默认使用的表，负责对流入、流出本机的数据包进行过滤，该表中定义了3个链：

**INPOUT** 负责过滤所有目标地址是本机地址的数据包，就是过滤进入主机的数据包。

**FORWARD** 负责转发流经本机但不进入本机的数据包，起到转发的作用。

**OUTPUT** 负责处理所有源地址是本机地址的数据包，就是处理从主机发出去的数据包。