1. **iptables 之-m -state**

转载 2015年11月12日 17:54:44

Iptables参数

-m state --state <状态>

有数种状态，状态有：

▪ INVALID：无效的封包，例如数据破损的封包状态

▪ ESTABLISHED：已经联机成功的联机状态；

▪ NEW：想要新建立联机的封包状态；

▪ RELATED：这个最常用！表示这个封包是与我们主机发送出去的封包有关， 可能是响应封包或者是联机成功之后的传送封包！这个状态很常被设定，因为设定了他之后，只要未来由本机发送出去的封包，即使我们没有设定封包的 INPUT 规则，该有关的封包还是可以进入我们主机， 可以简化相当多的设定规则。

**实验1：**

允许 ICMP 封包与允许已建立的联机通过

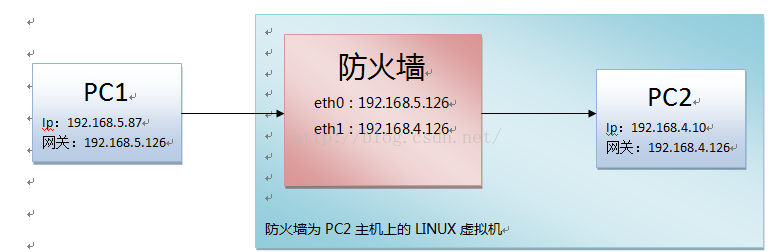
filter表中INPUT链为DROP，OUTPUT链为ACCEPT，

此时本机ping其他主机不通，在INPUT链中添加规则：

iptables -AINPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

本机可以ping其他主机，但是其他主机无法ping本机

**实验2:**

****

filter表中FORWARD链为DROP，nat表中链全部为ACCEPT

添加以下规则：

iptables -AFORWARD -d 192.168.4.10 -p icmp -j ACCEPT

iptables -AFORWARD -d 192.168.4.10 -p tcp --dport 80 -j ACCEPT

iptables -AFORWARD -d 192.168.4.10 -p tcp --dport 3389 -j ACCEPT

iptables -AFORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

PC1可顺利访问PC2上的80，3389端口。