iptables

防御SYN flood攻击:

```
iptables -A INPUT -p tcp --syn -m limit --limit 5/s -i eth0 -j ACCEPT
```

该条命令结果为，防火墙每秒中接受5个syn包，超过的syn包直接被丢弃。

允许外网访问内网的Web服务器:

```
iptables -A FORWARD -s 0/0 -i eth0 -d 192.168.1.58 -o eth1 -p TCP --sport
1024:65535 -m multiport --dport 80,443 -j ACCEPT
```

只有已经建立的连接才能通过:

```
iptables -A FORWARD -d 0/0 -o eth0 -s 192.168.1.58 -i eth1 -p TCP    -m state
--state ESTABLISHED -j ACCEPT
```

Adding a stateful rule

```
iptables -P INPUT DROP
iptables -A INPUT -i ! eth1 -j ACCEPT
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Practice

- Disable to be pinged, enable to ping
- To limit the number of pings
- To change the source IP of a ping packet sent out from our machine

```
sudo iptables -A INPUT -p icmp --icmp-type 8 -j DROP

iptables -P INPUT DROP
iptables -A INPUT -I eth0 -p icmp -m state --state ESTABLISH,RELATED -j ACCEPT

iptables -A INPUT -p icmp --icmp-type echo-request -m limit --limit 30/min --
limit-burst 8 -j ACCEPT
iptables -A INPUT -p icmp --icmp-type echo-request -j DROP
```

```
sudo iptables -t nat -A POSTROUTING -p icmp --icmp-type 8 -j SNAT --to-source
192.168.137.131
```

To act as firewall

```
sudo iptables -t nat -A PREROUTING -p tcp --dport 8123 -j DNAT --to
192.168.141.235:80

sudo iptables -t nat -A POSTROUTING -p tcp -s 192.168.141.235 --sport 80 -j
SNAT --to 192.168.141.226:8123
```

Netfilter

Netfilter是Linux 2.4.x引入的一个子系统，它作为一个通用的、抽象的框架，提供一整套的hook函数的管理机制，使得诸如数据包过滤、网络地址转换(NAT)和基于协议类型的连接跟踪成为了可能。 这幅图，很直观的反应了用户空间的iptables和内核空间的基于Netfilter的ip_tables模块之间的关系和其通讯方式，以及Netfilter在这其中所扮演的角色。