

iptables

iptables是运行在用户空间的一个应用软件，通过接口控制内核模块netfilter模块，以达到对流入流出及转发的数据报文进行过滤及其他操作的功能。netfilter是在内核空间实现防火墙功能的框架。事实上iptables不具有任何防火墙的功能，它只是运行在前端的一个程序，帮助用户制定管理防火墙规则的规则管理器。

netfilter

netfilter在内核中使用5个钩子函数实现防火墙功能，这五个钩子对应5条链。可以理解成这五个钩子在内核5个不同的位置进行看守，对数据过滤或流向等进行监控以及做出动作。通过在每个位置制定相应的规则，对报文流经的每个位置进行检查过滤，达到防火墙的功能。

链

1. **PREROUTING**: 路由前决策，报文最先到达主机匹配的位置
2. **INPUT**: 报文到达本机经过的位置
3. **FORWARD**: 由本机转发的报文流经的位置
4. **OUTPUT**: 由本机发出的数据报文经过的位置
5. **POSTROUTING**: 第二次路由决策，报文从本机流出的最后位置

表

每条链上制定多条规则，而这些规则的功能是不尽相同的。根据功能不同，通常iptables中又分为有四张表。具有相同功能的规则写入不同的链中，由这些具有相同功能的规则组成的链组成表。

iptables中的四表及功能：

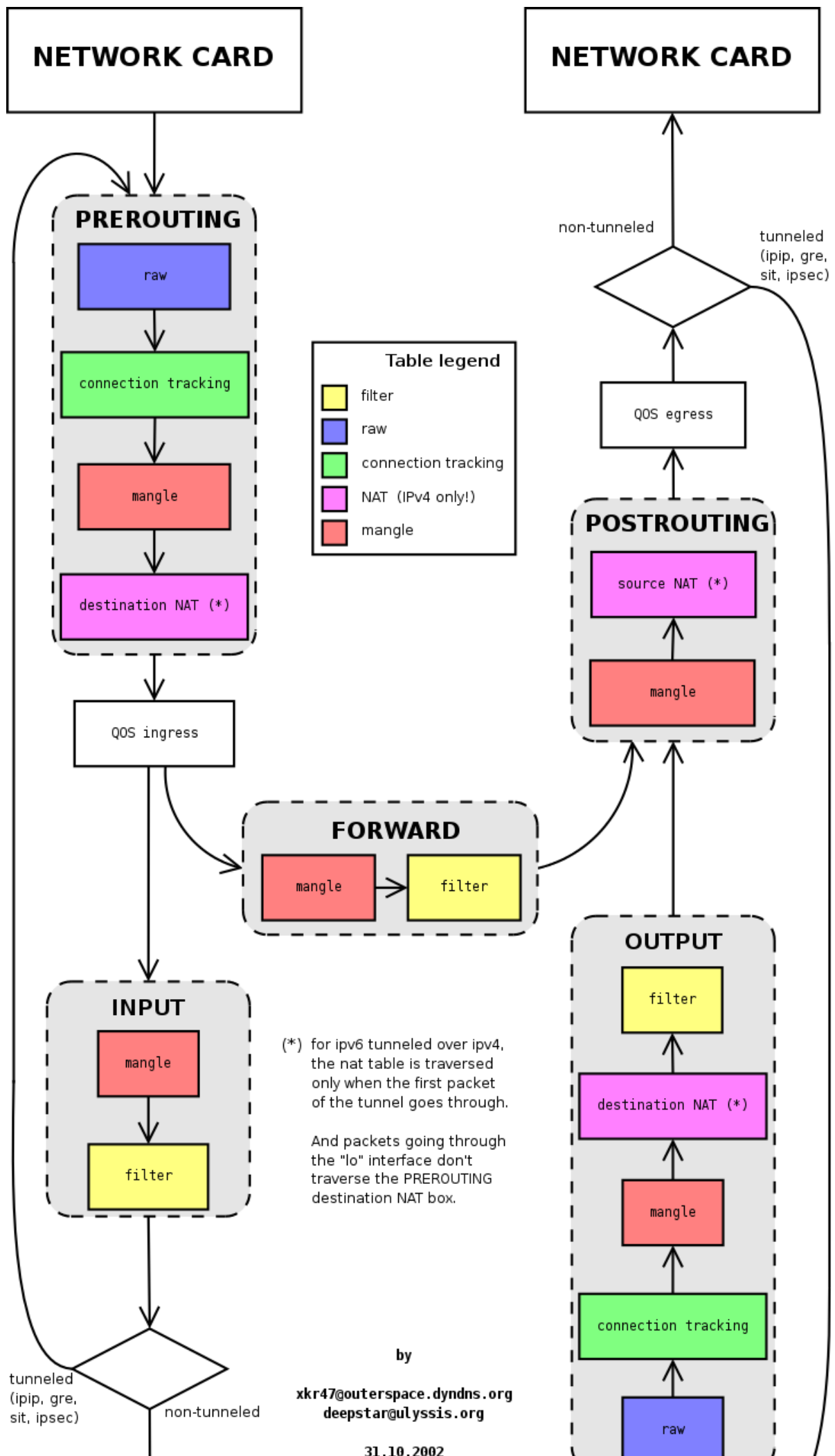
1. **filter**: 对数据包进行过滤，并作出动作
2. **nat**: 地址转换
3. **mangle**: 拆除报文、修改、封装报文

4. **raw**: 关闭nat表上启用的连接追踪功能，在非常繁忙服务器上要关闭连接追踪功能，否则可能会造成占用大量内存

对报文的处理动作(target)

1. **ACCEPT**: 允许报文通过
2. **DROP**: 丢弃报文，不做响应
3. **REJECT**: 拒绝报文通过，并明确响应请求方拒绝通过
4. **SNAT**: 源地址转换
5. **DNAT**: 目标地址转换
6. **MASQUERADE**: 地址伪装SNAT，例如将内网地址转换成一个对外的一个IP

规则匹配顺序|报文流向|各功能实现位置|各位置可以使用的功能



图片来源: <http://www.adminsehow.com/2011/09/iptables-packet-traverse-map/>

