相关概念

防火墙

> 防火墙最基本的功能就是隔离网络，通过将网络划分成不同的区域（通常情况下称为ZONE），制定出不同区域之间的访问控制策略来控制不同信任程度区域间传送的数据流。防火墙可以硬件防火墙也可以是软件防火墙。常见的防火墙架构有：主机防火墙、网络防火墙、硬件防火墙。主机防火墙在本主机的内核 TCP/IP 协议栈实现，网络防火墙在一个网络内的出口位置由专用的硬件对流经网络的数据报文进行过滤处理。硬件防火墙在专用的硬件级别实现部分防火墙功能，另一个部分由软件实现。

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 netfiler 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

> netfiter 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。netfilter 具有拒绝任何报文的经过本机的功能，而需要数据报文流经本地，则需要

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各不相同。根据功能的不同，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：

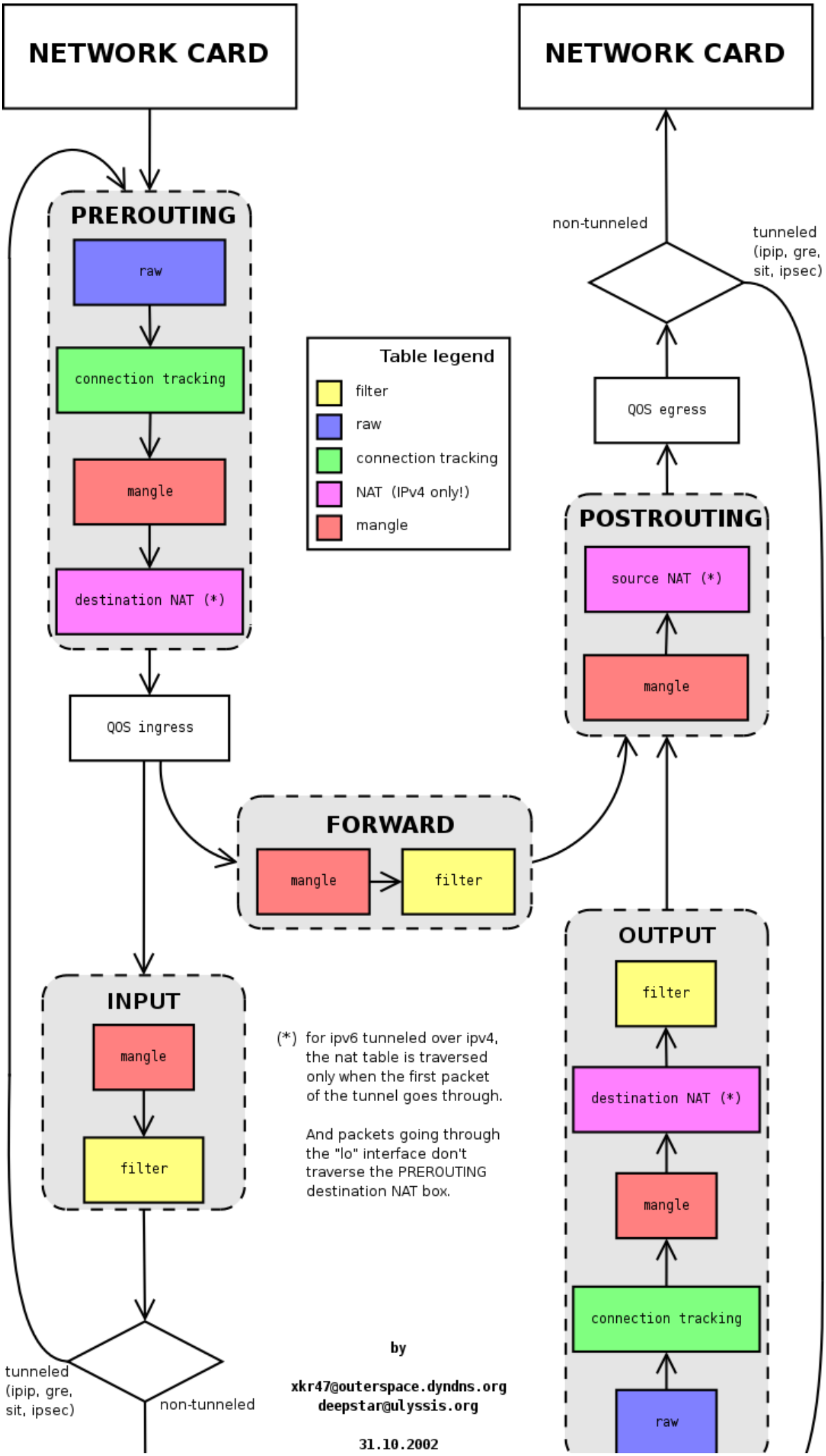
1. **filter：** 对数据包进行过滤，并作出动作
2. **nat：** 网络地址转换
3. **mange：** 拆除报文、修改报文、封装报文
4. **raw：** 关闭nat表上启用的连接追踪功能，在非常繁忙服务器上要关闭连接追踪功能，否则可能会造成占用大量内存

对报文的处理动作(target)

> 对报文可以有匹配条件和处理动作，匹配条件有基本匹配条件和扩展匹配条件。处理动作有内建处理动作和自动义处理动作，下列是内建处理动作。

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


NETWORK CARD
NETWORK CARD
PREROUTING
raw
connection tracking
mangle
destination NAT (*)
QOS ingress
Table legend
filter
raw
connection tracking
NAT (IPv4 only!)
mangle
non-tunneled
tunneled (ipip, gre, sit, ipsec)
QOS egress
POSTROUTING
source NAT (*)
mangle
FORWARD
mangle
filter
INPUT
mangle
filter
OUTPUT
filter
destination NAT (*)
mangle
connection tracking
raw
tunneled (ipip, gre, sit, ipsec)
non-tunneled
(*) for ipv6 tunneled over ipv4, the nat table is traversed only when the first packet of the tunnel goes through.
And packets going through the "lo" interface don't traverse the PREROUTING destination NAT box.
by
xkr47@outerspace.dyndns.org
deepstar@ulyssis.org
31.10.2002

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