ebtables 和 iptables 类似，都是 Linux 系统下网络数据包过滤的配置工具。既然称之为配置工具，就是说过滤功能是由内核底层提供支持的，这两个工具只是负责制定过滤的 rules.

ebtables 即是以太网桥防火墙，以太网桥工作在数据链路层，ebtables 来过滤数据链路层数据包。 2.6 内核内置了 ebtables，要使用它必须先安装 ebtables 的用户空间工具（ebtables-v2.0.6），安装完成后就可以使用 ebtables 来过滤网桥的数据包。 参照用户实际要求，设置 ebtables 规则如下：

1:对所有的数据包默认通过

2:分清楚源地址和目的地址和源端口和目的端口

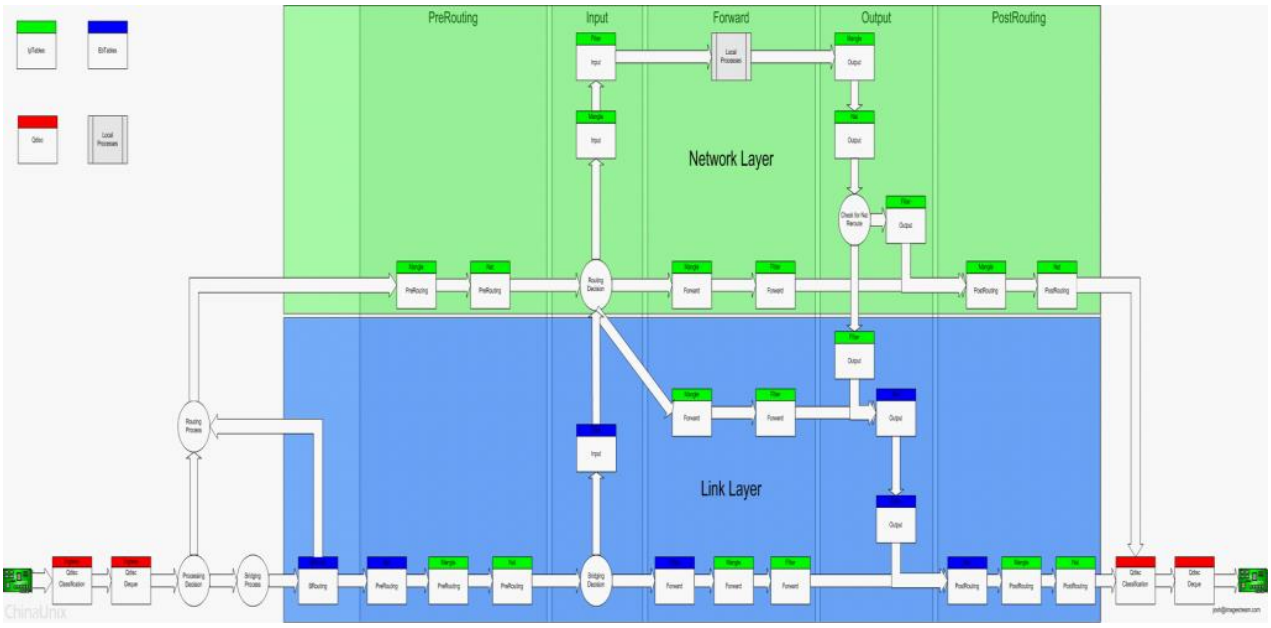
3:对 TCP,UDPP 数据包分别过滤

ebtables 是主要是控制数据链路层的,在内核中，ebtables 的数据截获点比 iptables 更“靠前”，它获得的数据更“原始”，ebtables 多用于桥模式，比如控制 VLAN ID 等。

ebtables 就像以太网桥的 iptables。 iptables 不能过滤桥接流量，而 ebtables 可以。ebtables 不适合作为 Internet 防火墙。

一、过滤时机

要了解过滤时机，首先得了解网络数据包进入网卡后，在系统中的转换流程，见下图：



从上图可以看到数据包从进入到离开系统，要经过 PreRoute，Input，Forward，Output，PostRoute 这五个阶段。每个阶段中包括了一些节点，每个节点就是一个过滤时机。当数据包行进到某个节点时，系统就是检测对应节点的过滤规则并进行过滤。从图中还可以发现，对于每个阶段，ebtables 的过滤时机都比 iptables 要早。

二、ebtables 配置

ebtables 的配置分为表、链和规则三级。

1. 表

表是内置且固定的，共有三种: filter, nat, broute，用-t 选项指定。最常用的就是 filter 了，所以不设-t 时默认就是这个表。nat 用于地址转换，broute 用于以太网桥。

2. 链

链有内置和自定义两种 。不同的表内置的链不同，这个从数据包的流程图中就可以看出来。所谓自定义的链也是挂接在对应的内置链内的，使用-j 让其跳转到新的链中。

3. 规则

每个链中有一系列规则，每个规则定义了一些过滤选项。每个数据包都会匹配这些项，一但匹配成功就会执行对应的动作。

所谓动作，就是过滤的行为了。有四种，ACCEPT，DROP，RETURN 和 CONTINUE。常用的就是 ACCEPT 和 DROP，另两种就不细述了。

Ebtables 使用规则如下：

ebtables [-t table] -[ADI] chain rule-specification [match-extensions] [watcher-extensions]

-t table :一般为 FORWARD 链。

- ADI：A 添加到现有链的末尾；D 删除规则链（必须指明规则链号）；I 插入新的规则链（必须指明规则链号）。

-P:规则表的默认规则的设置。可以 DROP,ACCEPT,RETURN。

-F:对所有的规则表的规则链清空。

-L:指明规则表。可加参数，--Lc,--Ln

-p:指明使用的协议类型，ipv4,arp 等可选（使用时必选）详情见/etc/ethertypes

--ip-proto:IP 包的类型，1 为 ICMP 包，6 为 TCP 包，17 为 UDP 包，在/etc/protocols 下有详细说明

--ip-src:IP 包的源地址

--ip-dst:IP 包的目的地址

--ip-sport:IP 包的源端口

--ip-dport:IP 包的目的端口

-i:指明从那片网卡进入

-o:指明从那片网卡出去

三、ebtables 基本命令

有了上面的简单介绍，再熟悉一些基本命令就可以使用了。

1. 列表：

ebtables -L

ebtables -L –Lc , 查看各 rule 的匹配次数以及字节数

2. 新建/删除链

ebtables -N <chain_name>

ebtables -X <chain_name>

3. 新建规则

ebtables -A <chain_name> [rules]

[rules]有几种

-s 源 MAC -d 目标 MAC -i 入接口 -o 出接口

命令示例：

ebtables -P FORWARD ACCEPT

ebtables -P INPUT ACCEPT

ebtables -P OUTPUT ACCEPT

ebtables -F

ebtables -A FORWARD -p ipv4 -i eth0/eth1 --ip-proto (6/17) --ip-dst(目的 IP) --ip-dport(目的端口) -j DROP

ebtables -A FPRWARD -p ipv4 -i eth0/eth1 --ip-proto (7/17) --ip-src(源

IP) --ip-sport(源端口) -j DROP