

iptables详解（1）：iptables概念 (<https://www.zsythink.net/archives/1199>)

这篇文章会尽量以通俗易懂的方式描述iptables

(<https://www.zsythink.net/archives/tag/iptables/>)的相关概念，请耐心的读完它。

防火墙相关概念

此处先描述一些相关概念。

从逻辑上讲。防火墙可以大体分为主机防火墙和网络防火墙。

主机防火墙：针对于单个主机进行防护。

网络防火墙：往往处于网络入口或边缘，针对于网络入口进行防护，服务于防火墙背后的本地局域网。

网络防火墙和主机防火墙并不冲突，可以理解为，网络防火墙主外（集体），主机防火墙主内（个人）。

从物理上讲，防火墙可以分为硬件防火墙和软件防火墙。

硬件防火墙：在硬件级别实现部分防火墙功能，另一部分功能基于软件实现，性能高，成本高。

软件防火墙：应用软件处理逻辑运行于通用硬件平台之上的防火墙，性能低，成本低。



那么在此处，我们就来聊聊Linux的iptables

iptables其实不是真正的防火墙，我们可以把它理解成一个客户端代理，用户通过iptables这个代理，将用户的安全设定执行到对应的“安全框架”中，这个“安全框架”才是真正的防火墙，这个框架的名字叫**netfilter**

netfilter才是防火墙真正的安全框架（framework），netfilter位于内核空间。

iptables其实是一个命令行工具，位于用户空间，我们用这个工具操作真正的框架。

netfilter/iptables（下文中简称为iptables）组成Linux平台下的包过滤防火墙，与大多数的Linux软件一样，这个包过滤防火墙是免费的，它可以代替昂贵的商业防火墙解决方案，完成封包过滤、封包重定向和网络地址转换（NAT）等功能。

Netfilter是Linux操作系统核心层内部的一个数据包处理模块，它具有如下功能：

网络地址转换(Network Address Translate)

数据包内容修改

以及数据包过滤的防火墙功能

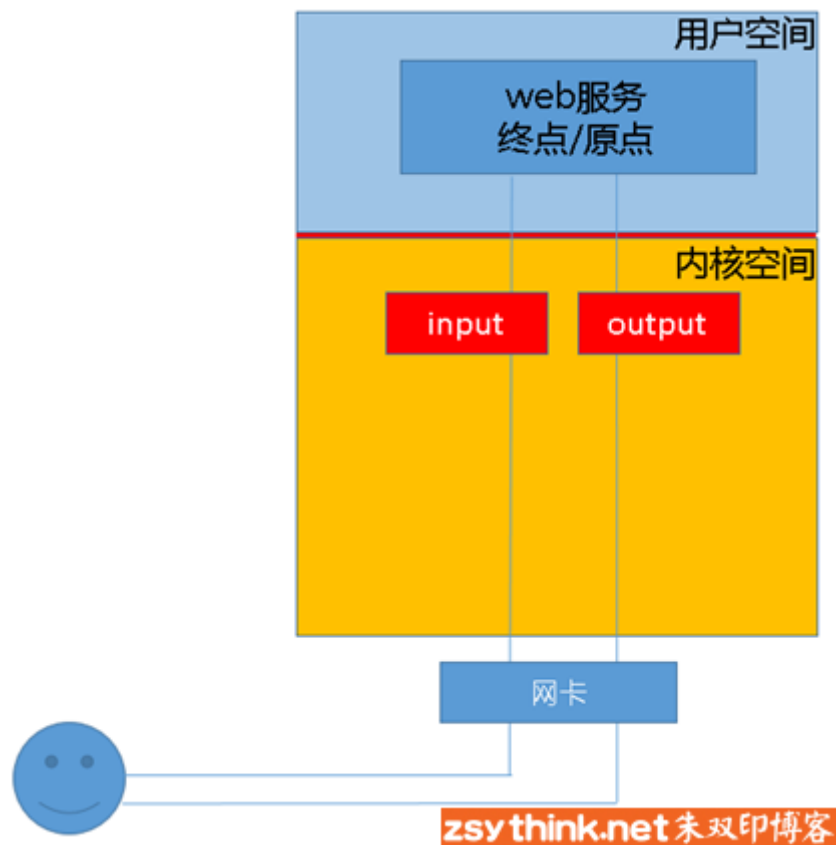
所以说，虽然我们使用`service iptables start`启动iptables”服务”，但是其实准确的来说，iptables并没有一个守护进程，所以并不能算是真正意义上的服务，而应该算是内核提供的功能。

iptables基础

我们知道iptables是按照规则来办事的，我们就来说说规则（rules），规则其实就是网络管理员预定义的条件，规则一般的定义为“如果数据包头符合这样的条件，就这样处理这个数据包”。规则存储在内核空间的信息包过滤表中，这些规则分别指定了源地址、目的地址、传输协议（如TCP、UDP、ICMP）和服务类型（如HTTP、FTP和SMTP）等。当数据包与规则匹配时，iptables就根据规则所定义的方法来处理这些数据包，如放行（accept）、拒绝（reject）和丢弃（drop）等。配置防火墙的主要工作就是添加、修改和删除这些规则。

这样说可能并不容易理解，我们来换个容易理解的角度，从头说起。

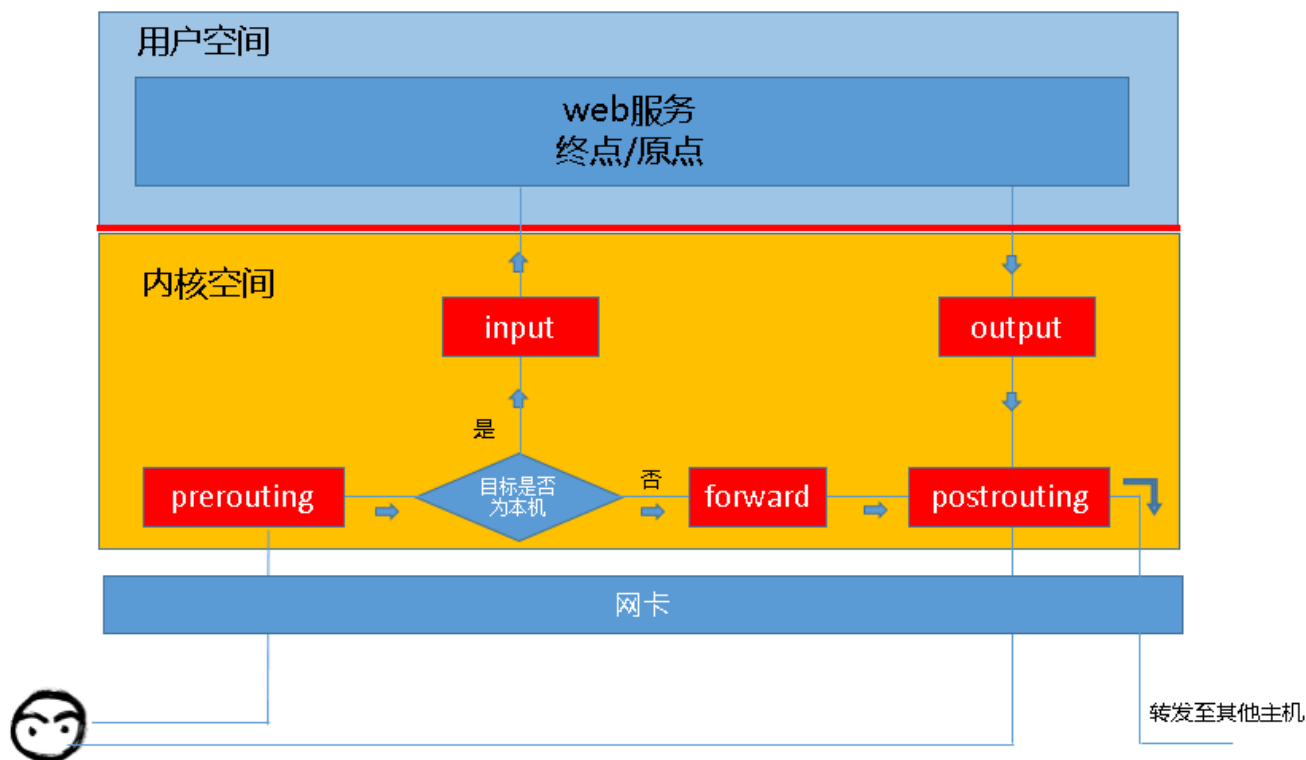
当客户端访问服务器的web服务时，客户端发送报文到网卡，而tcp/ip协议栈是属于内核的一部分，所以，客户端的信息会通过内核的TCP协议传输到用户空间中的web服务中，而此时，客户端报文的目标终点为web服务所监听的套接字（IP：Port）上，当web服务需要响应客户端请求时，web服务发出的响应报文的目标终点则为客户端，这个时候，web服务所监听的IP与端口反而变成了原点，我们说过，netfilter才是真正的防火墙，它是内核的一部分，所以，如果我们想要防火墙能够达到“防火”的目的，则需要在内核中设置关卡，所有进出的报文都要通过这些关卡，经过检查后，符合放行条件的才能放行，符合阻拦条件的则需要被阻止，于是，就出现了input关卡和output关卡，而这些关卡在iptables中不被称为“关卡”，而被称为“链”。



其实我们上面描述的场景并不完善，因为客户端发来的报文访问的目标地址可能并不是本机，而是其他服务器，当本机的内核支持IP_FORWARD时，我们可以将报文转发给其他服务器，所以，这个时候，我们会提到iptables中的其他“关卡”，也就是其他“链”，他们就是“路由前”、“转发”、“路由后”，他们的英文名是

PREROUTING、FORWARD、POSTROUTING

也就是说，当我们启用了防火墙功能时，报文需要经过如下关卡，也就是说，根据实际情况的不同，报文经过“链”可能不同。如果报文需要转发，那么报文则不会经过input链发往用户空间，而是直接在内核空间中经过forward链和postrouting链转发出去的。



zsythink.net 朱双印博客

所以，根据上图，我们能够想象出某些常用场景中，报文的流向：

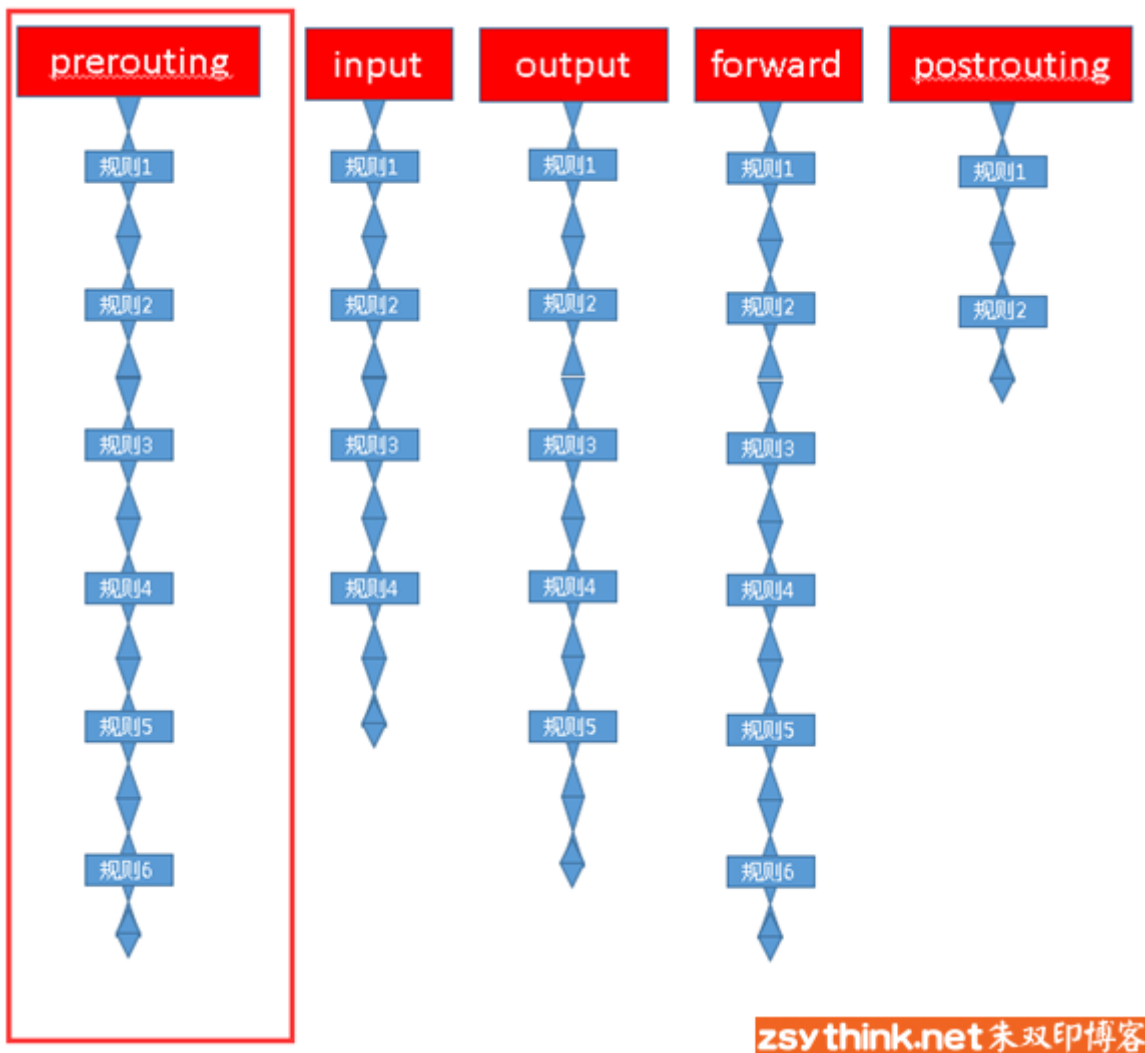
到本机某进程的报文：PREROUTING → INPUT

由本机转发的报文：PREROUTING → FORWARD → POSTROUTING

由本机的某进程发出报文（通常为响应报文）：OUTPUT → POSTROUTING

链的概念

现在，我们想象一下，这些“关卡”在iptables中为什么被称作“链”呢？我们知道，防火墙的作用就在于对经过的报文匹配“规则”，然后执行对应的“动作”，所以，当报文经过这些关卡的时候，则必须匹配这个关卡上的规则，但是，这个关卡上可能不止有一条规则，而是有很多条规则，当我们把这些规则串到一个链条上的时候，就形成了“链”，所以，我们把每一个“关卡”想象成如下图中的模样，这样来说，把他们称为“链”更为合适，每个经过这个“关卡”的报文，都要将这条“链”上的所有规则匹配一遍，如果有符合条件的规则，则执行规则对应的动作。



表的概念

我们再想想另外一个问题，我们对每个“链”上都放置了一串规则，但是这些规则有些很相似，比如，A类规则都是对IP或者端口的过滤，B类规则是修改报文，那么这个时候，我们是不是能把实现相同功能的规则放在一起呢，必须能的。

我们把具有相同功能的规则的集合叫做“表”，所以说，不同功能的规则，我们可以放置在不同的表中进行管理，而iptables已经为我们定义了4种表，每种表对应了不同的功能，而我们定义的规则也都逃脱不了这4种功能的范围，所以，学习iptables之前，我们必须先搞明白每种表的作用。

iptables为我们提供了如下规则的分类，或者说，iptables为我们提供了如下“表”

filter表：负责过滤功能，防火墙；内核模块：iptables_filter

nat表：network address translation，网络地址转换功能；内核模块：iptable_nat

mangle表：拆解报文，做出修改，并重新封装 的功能；iptable_mangle

raw表：关闭nat表上启用的连接追踪机制；iptable_raw

也就是说，我们自定义的所有规则，都是这四种分类中的规则，或者说，所有规则都存在于这4张“表”中。

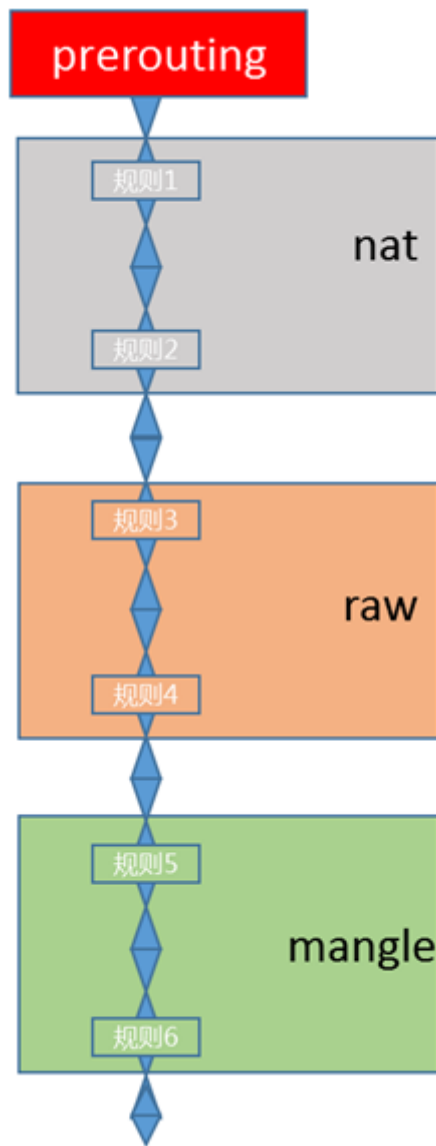
表链关系

但是我们需要注意的是，某些“链”中注定不会包含“某类规则”，就像某些“关卡”天生就不具备某些功能一样，比如，A“关卡”只负责打击陆地敌人，没有防空能力，B“关卡”只负责打击空中敌人，没有防御步兵的能力，C“关卡”可能比较NB，既能防空，也能防御陆地敌人，D“关卡”最屌，海陆空都能防。

那让我们来看看，每个“关卡”都有哪些能力，或者说，让我们看看每个“链”上的规则都存在于哪些“表”中。

我们还是以图为例，先看看prerouting“链”上的规则都存在于哪些表中。

注意：下图只用于说明prerouting链上的规则存在于哪些表中，并没有描述表的顺序。



这幅图是什么意思呢？它的意思是说，prerouting“链”只拥有nat表、raw表和mangle表所对应的功能，所以，prerouting中的规则只能存放于nat表、raw表和mangle表中。

那么，根据上述思路，我们来总结一下，每个“关卡”都拥有什么功能，

或者说，每个“链”中的规则都存在于哪些“表”中。

PREROUTING 的规则可以存在于：raw表，mangle表，nat表。

INPUT 的规则可以存在于：mangle表，filter表，（centos7中还有nat表，centos6中没有）。

FORWARD 的规则可以存在于：mangle表，filter表。

OUTPUT 的规则可以存在于：raw表mangle表，nat表，filter表。

POSTROUTING 的规则可以存在于：mangle表，nat表。

但是，我们在实际的使用过程中，往往是通过“表”作为操作入口，对规则进行定义的，之所以按照上述过程介绍iptables，是因为从“关卡”的角度更容易从入门的角度理解，但是为了以便在实际使用的时候，更加顺畅的理解它们，此处我们还要将各“表”与“链”的关系罗列出来，

表（功能）<--> 链（钩子）：

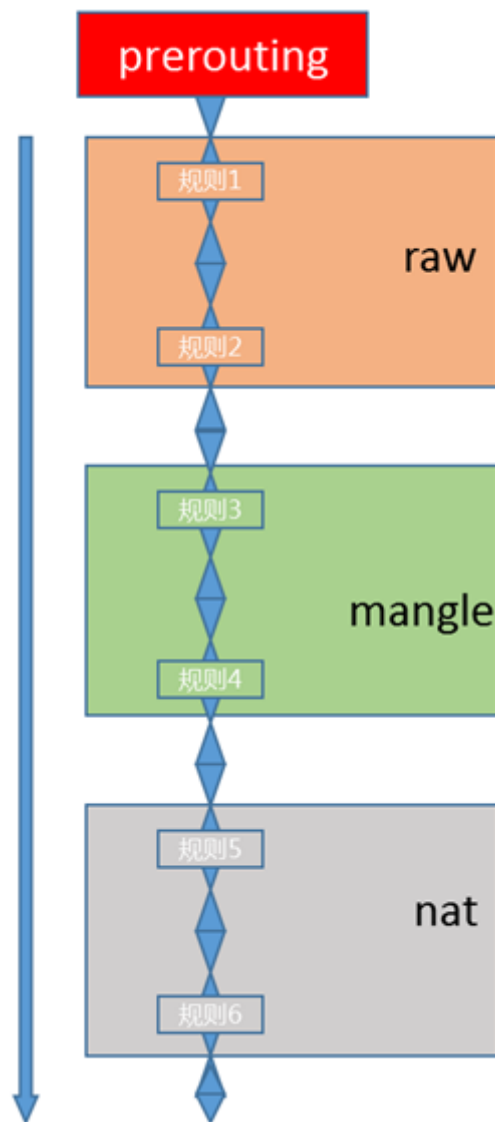
raw 表中的规则可以被哪些链使用：PREROUTING，OUTPUT

mangle 表中的规则可以被哪些链使用：PREROUTING，INPUT，FORWARD，OUTPUT，POSTROUTING

nat 表中的规则可以被哪些链使用：PREROUTING，OUTPUT，POSTROUTING（centos7中还有INPUT，centos6中没有）

filter 表中的规则可以被哪些链使用：INPUT，FORWARD，OUTPUT

其实我们还需要注意一点，因为数据包经过一个“链”的时候，会将当前链的所有规则都匹配一遍，但是匹配时总归要有顺序，我们应该一条一条的去匹配，而且我们说过，相同功能类型的规则会汇聚在一张“表”中，那么，哪些“表”中的规则会放在“链”的最前面执行呢，这时候就需要有一个优先级的問題，我们还拿prerouting“链”做图示。



prerouting链中的规则存放于三张表中，而这三张表中的规则执行的优先级如下：

raw → mangle → nat

但是我们知道，iptables为我们定义了4张“表”，当他们处于同一条“链”时，执行的优先级如下。

优先级次序（由高而低）：

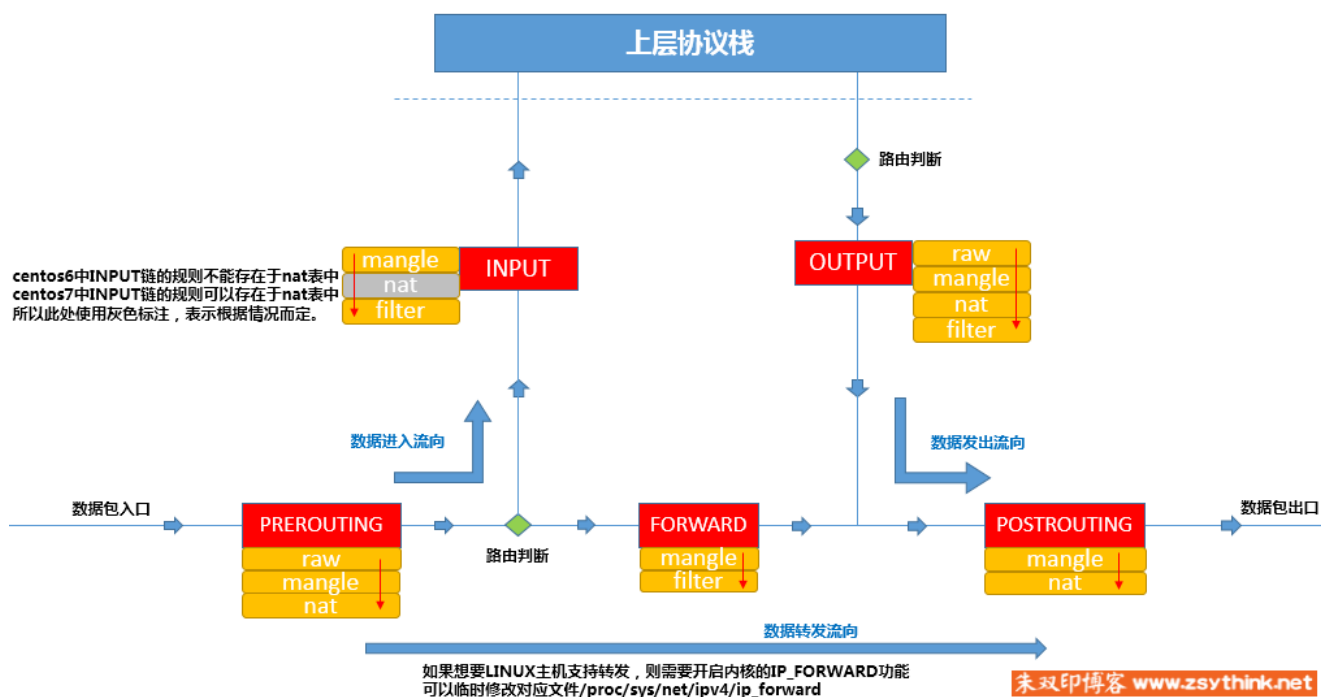
raw → mangle → nat → filter

但是我们前面说过，某些链天生就不能使用某些表中的规则，所以，4张表中的规则处于同一条链的目前只有output链，它就是传说中海陆空都能防守的关卡。

为了更方便的管理，我们还可以在某个表里面创建自定义链，将针对某个应用程序所设置的规则放置在这个自定义链中，但是自定义链接不能直接使用，只能被某个默认的链当做动作去调用才能起作用，我们可以这样想象，自定义链就是一段比较“短”的链子，这条“短”链子上的规则都是针对某个应用程序制定的，但是这条短的链子并不能直接使用，而是需要“焊接”在iptables默认定义链子上，才能被IPtables使用，这就是为什么默认定义的“链”需要把“自定义链”当做“动作”去引用的原因。这是后话，后面再聊，在实际使用时我们即可更加的明白。

数据经过防火墙的流程

结合上述所有的描述，我们可以将数据包通过防火墙的流程总结为下图：



我们在写Iptables规则的时候，要时刻牢记这张路由次序图，灵活配置规则。

我们将经常用到的对应关系重新写在此处，方便对应图例查看。

链的规则存放于哪些表中（从链到表的对应关系）：

PREROUTING 的规则可以存在于：raw表，mangle表，nat表。

INPUT 的规则可以存在于：mangle表，filter表，（centos7中还有nat表，centos6中没有）。

FORWARD 的规则可以存在于：mangle表，filter表。

OUTPUT 的规则可以存在于：raw表mangle表，nat表，filter表。

POSTROUTING 的规则可以存在于：mangle表，nat表。

表中的规则可以被哪些链使用（从表到链的对应关系）：

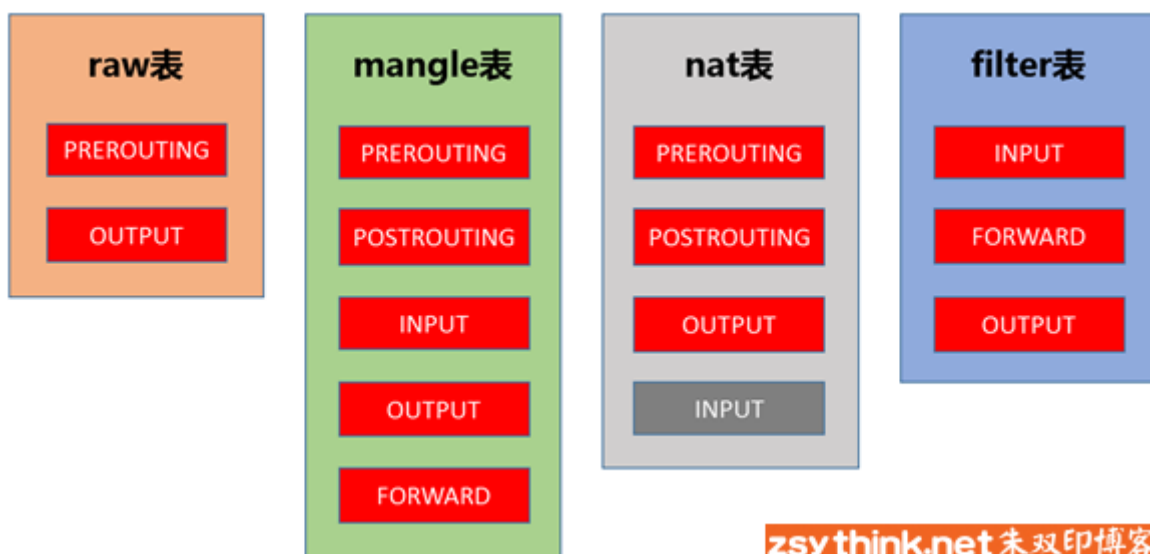
raw 表中的规则可以被哪些链使用：PREROUTING，OUTPUT

mangle 表中的规则可以被哪些链使用：PREROUTING，INPUT，FORWARD，OUTPUT，POSTROUTING

nat 表中的规则可以被哪些链使用：PREROUTING，OUTPUT，POSTROUTING（centos7中还有INPUT，centos6中没有）

filter 表中的规则可以被哪些链使用：INPUT，FORWARD，OUTPUT

下图中nat表在centos7中的情况就不再标明。



规则的概念

说了一圈又说回来了，在上述描述中我们一直在提规则，可是没有细说，现在说说它。

先说说规则的概念，然后再通俗的解释它。

规则：根据指定的匹配条件来尝试匹配每个流经此处的报文，一旦匹配成功，则由规则后面指定的处理动作进行处理；

那么我们来通俗的解释一下什么是iptables的规则，之前打过一个比方，每条“链”都是一个“关卡”，每个通过这个“关卡”的报文都要匹配这个关卡上的规则，如果匹配，则对报文进行对应的处理，比如说，你我二人此刻就好像两个“报文”，你我二人此刻都要入关，可是城主有命，只有器宇轩昂的人才可能入关，不符合此条件的人不能入关，于是守关将士按照城主制定的“规则”，开始打量你我二人，最终，你顺利入关了，而我已被拒之门外，因为你符合“器宇轩昂”的标准，所以把你“放行”了，而我不符合标准，所以没有被放行，其实，“器宇轩昂”就是一种“匹配条件”，“放行”就是一种“动作”，“匹配条件”与“动作”组成了规则。

了解了规则的概念，那我们来聊聊规则的组成部分,此处只是大概的将规则的结构列出，后面的文章中会单独对规则进行总结。

规则由匹配条件和处理动作组成。

匹配条件

匹配条件分为基本匹配条件与扩展匹配条件

基本匹配条件：

源地址Source IP，目标地址 Destination IP

上述内容都可以作为基本匹配条件。

扩展匹配条件：

除了上述的条件可以用于匹配，还有很多其他的条件可以用于匹配，这些条件泛称为扩展条件，这些扩展条件其实也是netfilter中的一部分，只是以模块的形式存在，如果想要使用这些条件，则需要依赖对应的扩展模块。

源端口Source Port, 目标端口Destination Port

上述内容都可以作为扩展匹配条件

处理动作

处理动作在iptables中被称为target（这样说并不准确，我们暂且这样称呼），动作也可以分为基本动作和扩展动作。

此处列出一些常用的动作，之后的文章会对它们进行详细的示例与总结：

ACCEPT：允许数据包通过。

DROP：直接丢弃数据包，不给任何回应信息，这时候客户端会感觉自己的请求泥牛入海了，过了超时时间才会有反应。

REJECT：拒绝数据包通过，必要时会给数据发送端一个响应的信息，客户端刚请求就会收到拒绝的信息。

SNAT：源地址转换，解决内网用户用同一个公网地址上网的问题。

MASQUERADE：是SNAT的一种特殊形式，适用于动态的、临时会变的ip上。

DNAT：目标地址转换。

REDIRECT：在本机做端口映射。

LOG：在/var/log/messages文件中记录日志信息，然后将数据包传递给下一条规则，也就是说除了记录以外不对数据包做任何其他操作，仍然让下一条规则去匹配。

小结

iptables的实际操作我们会另外总结为其他文章，iptables系列文章列表直达链接如下：

iptables零基础快速入门系列

(<https://www.zsythink.net/archives/tag/iptables/>)


好了，iptables的概念暂时总结到这里，懂得概念之后，再结合实际命令去练习，搞定iptables绝对妥妥的。


最后说一句，客官您的**评论、收藏、推荐**是我写博客的最大动力，希望亲以后多捧场哦，么么哒

~~~~~

 评论 共357条

有什么想要探讨的吗？

 提交评论



aced0005

 0

非常棒的博客，感谢作者

4天前



jhonsnow

 0

给力 通俗易懂

27天前



xxx

👍 0



45天前



Snow

👍 0

大佬讲的通俗易懂！！！！👍

1月前



牛蛙儿

👍 0

学docker k8s, iptables这块必须学啊

3月前



wkj

👍 2

大佬写的太好了，什么时候能出tcpdump的教学👉

3月前



zmouc

👍 0

@wewen

很明显，你的第35行配置里面有3个--to-destination，删除掉其中两个就可以了

~~~~~

```
]# iptables-save > /etc/sysconfig/iptables.bak
```

```
]# iptables-restore < /etc/sysconfig/iptables.bak
```

```
iptables-restore v1.4.21: Bad IP address ""
```

```
Error occurred at line: 35
```

```
Try 'iptables-restore -h' or 'iptables-restore --help' for more information.
```

执行 iptables-save 后执行 iptables-restore 报错，不知道什么原因，看提示的 35 行有问题，看到 iptables.bak 第 35 行如下，也没看出什么问题

```
35 -A KUBE-SEP-6EN3O4ZLERHKTN3D -p tcp -m comment --comment
```

```
"default/kubernetes:https" -m tcp -j DNAT --to-destination --to-destination --to-destination 0.0.0.0 -
```

```
-persistent
```

有其他大佬遇到过吗？

4月前



码农

👍 1

大佬，您这讲的太好了，浅显易懂，完爆大学教授们，建议可以结集出书，市面上同类型的书就要下架了

6月前



33

👍 0

生动形象，写的真的好

6月前



朱泽想

👍 0

牛哇牛哇，大佬文章用词生动形象，往往让人不容易理解的原理看完有种竟然如此简单的错觉，文档质量和格式都是精品中的精品，向大佬看齐(ง •_•)ง

6月前



xhaiben

👍 0

写的真好呀👍

7月前



happy

👍 0

只能说讲的厉害

7月前



ilymyself521

👍 1

我有一个疑问，本机是指什么？是指软路由本身么，还是软路由后面的局域网？那我在软路由局域网接入一个NAS服务器，从外界访问NAS是属于转发呢？还是input和output链？如果是转发链按照介绍就不需要经过input和output链，可我为什么在安全区域里面把入站和出站改为拒绝后，只保留转发，端口转发就失效了呢？这点搞不明白，希望有大神给解惑一下！

7月前



cirry

👍 0

没啥好说的，只能说牛皮

7月前



bbbb

👍 1

流畅清晰。像一个主持人把整个谈话引导得流畅清晰，又不露痕迹。功力👍

7月前



龟龟

👍 1

太厉害了！感觉比网上那些大牛讲的都要清晰啊

8月前



LKarrie

👍 0

牛逼，收获颇丰，谢谢你的文章！

9月前



爱上学习

👍 1

膜拜大佬，跟着大佬学习

9月前



小管

👍 3

解释的太生动了，刷哔哩哔哩，有个人照着你这个文章说的15分钟，最近搭建kubernetes 网络各种出问题，必须的学习iptables了

9月前



小偶丁丁

👍 1

牛哇牛哇，大佬文章用词生动形象，往往让人不容易理解的原理看完有种竟然如此简单的错觉，文档质量和格式都是精品中的精品，向大佬看齐(ง •̀_•́)ง

9月前



朱双印 (<https://www.zsythink.net/archives/author/1>) 作者

👍 0

兄弟，你和“叫我去学习”什么关系，评论咱就别复制了~😂，

9月前 @小偶丁丁



ggl

👍 0

从新温习一遍

10月前



学习

👍 0

mark一下

10月前



日复一日

👍 0

钉...打卡

10月前



汤姆猫

👍 1

全网讲解IPTABLES最清楚的，没有之一！

10月前



Walter

👍 0

大佬公众号多少

11月前



看到我请叫我去学习

👍 1

牛哇牛哇，大佬文章用词生动形象，往往让人不容易理解的原理看完有种竟然如此简单的错觉，文档质量和格式都是精品中的精品，向大佬看齐(ง •̀_•́)ง

11月前



朱双印 (<https://www.zsythink.net/archives/author/1>) 作者

👍 0

兄弟，看到你了，一起学习去啊~

11月前 @看到我请叫我去学习



Coco

👍 0

太牛了，直接、清晰！

最近在学docker和k8s，iptables 这块内容真是看这一篇足矣。4表5链一下就明白其间关系了

12月前



朱双印 (<https://www.zsythink.net/archives/author/1>) 作者

👍 0

博客中有docker的文章，可以一起看了 😊

12月前 @Coco



wewin

👍 0

```
]# iptables-save > /etc/sysconfig/iptables.bak
]# iptables-restore < /etc/sysconfig/iptables.bak
iptables-restore v1.4.21: Bad IP address ""
```

Error occurred at line: 35

Try `iptables-restore -h' or 'iptables-restore --help' for more information.

执行 iptables-save 后执行 iptables-restore 报错，不知道什么原因，看提示的 35 行有问题，看到 iptables.bak 第 35 行如下，也没看出什么问题

```
35 -A KUBE-SEP-6EN3O4ZLERHKTN3D -p tcp -m comment --comment
"default/kubernetes:https" -m tcp -j DNAT --to-destination --to-destination --to-destination 0.0.0.0 -
-persistent
```

有其他大佬遇到过吗？

1年前



aliao

👍 0

路由上的ACL也是差不多，根据规则逐条匹配

1年前



kaikai1988

👍 0

好文章。最近学习云原生，对这部分概念必须要掌握了。

1年前



youcoward

👍 0

这也太清晰了吧！！！！！！！！

1年前



zz

👍 1

写的很清晰，少走弯路

1年前



小和完完

👍 0

大牛，厉害厉害厉害，真的是很棒的分享，感谢博主分享

1年前



Demo

👍 0

新手一看就能入门理解了,真牛哇

1年前



Wonder

👍 0

学习，谢谢笔者。关注公众号了。

1年前



tyler

👍 0

重于遇到了一个把链和表的概念讲明白的文章了，感谢博主分享！

1年前



麦卡鲁

👍 2

有没有更好的办法来理解那一张表可以被哪些链引用呢？这个感觉死记硬背不好记，还是得从原理上理解。

1年前



苹果

👍 2

看第二遍了，清晰明了，真正的好文。

1年前



无恒

👍 2

我又来看一遍

2年前



kindle

👍 2

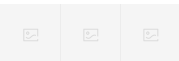
太棒了，谢谢大佬

2年前



诸葛孔明

👍 0



2年前



yqs

👍 1

很好得文章，收益很多

2年前



sknown

👍 0

同一链的是与逻辑？

2年前



华仔

👍 2

收货很多，感谢作者

2年前



3ge3.cn

👍 1

通俗易懂，一看就明白

2年前



卫星

👍 0

写得很好，收获很多，谢谢

2年前



123

👍 0

面对赞吧😁

2年前



luckyboy

👍 0

受益匪浅

第一次看到讲解的这么通透的文章

2年前



hell

👍 0

讲得很好，通俗易懂，目前看过最好的入门文章！

2年前



FishTHU

👍 0

讲得太好了，给你点赞👍

2年前



jmuchch

👍 0

精致的信息！

2年前



xsyxt

👍 0

感谢大佬，收藏祝贺

2年前



SEA_HORIZON

👍 0

谢了，大佬！

2年前



wjg

👍 1

太牛了，大佬

2年前



billy

👍 2

提点意见，最后那个处理动作，恰恰忽略了在透明代理实作中，使用最广泛的几个动作：return, mark

2年前



zfz

👍 0

辛苦了。非常受用

2年前



HUANGF

👍 0

感谢分享 受教了

2年前



木白

👍 0

写得太好了，第一次这么清晰的理解iptables

2年前



马化腾

👍 17

明天来我公司上班

2年前



Stephen

👍 1

写的超级好，我看前面十来行我就收藏了，牛皮

2年前



jtr109

👍 0

感谢分享，书写条理非常清晰，易于理解。

2年前



leesirc

👍 0

爱了，爱了，真的是爱了

2年前



哈哈

👍 0

大牛，厉害厉害厉害，真的是很棒的分享，感谢博主分享

2年前



一只程序媛

👍 0

很棒的分享，感谢博主



2年前



MR.Song

👍 0

爱了，被吸粉了

2年前



Rayson

👍 1

终于看完了，回来留个言打个卡。想问问博主会不会出一个firewalld的详解？

2年前



admin

👍 3

牛皮，网上的其他文章都是渣渣。

深入浅出，通俗易懂。

2年前



Nues

👍 0

写的通俗易懂

2年前



面对疾风吧

👍 0

好好好不错哦

2年前



迪丽热巴

👍 15

写得好，想叫你爸爸

2年前



桂花烧香

👍 1

写的真好，点赞

2年前



kiwill

👍 1

匹配规则应该是最小匹配

2年前



阿隆索打飞机

👍 1

五条链+四张表

2年前



兰陵笑笑生

👍 0

666666

2年前



bigdaxigua

👍 2

看了博主的很多文章，感觉讲的很通俗易懂，只要认真的看完每个章节，都会收获不小

2年前



砂子

👍 2

受教了。受教了。

2年前



FANPEI

👍 3

先讲链，后讲表，这么一讲，我一下子就豁然开朗了！这表达能力是真的厉害，造福！

2年前



mess

👍 4

讲的非常好。赞。

2年前



hhhhhh

👍 4

五个组件+4种表，全局观一下子有了。爆赞

2年前



Richard

👍 1

想请教个额外的问题，博主的博客是怎么搭建的，学习学习经验

2年前



LF

👍 1

太厉害了, 在别人那里看的云里雾里, 一看这个马上就理解了

2年前



BG

👍 0

讲的很好，感谢！

2年前



qixy

👍 0

写的清晰明了，很赞。

2年前



KID-Loong

👍 0

您好！新年好！博主的文章浅显易懂，很荣幸可以拜读，受益匪浅！该篇文章中有个疑问：在数据包流经的过程中，第二次的路由选择，到底是在output链前还是后呢？博主发的图是在output前，但这个在网上到底是在其前还是在其后都各有说法，不知博主可否解惑

2年前



朱双印 (<https://www.zsythink.net/archives/author/1>) 作者

👍 1

参考一下这篇文章，会有帮助，加油

https://wiki.nftables.org/wiki-nftables/index.php/Netfilter_hooks (https://wiki.nftables.org/wiki-nftables/index.php/Netfilter_hooks)

2年前 @KID-Loong



0-0

👍 0

读可赏心，观可悦目

2年前



非著名程序员

👍 0

写的有个性，不人云亦云！！

2年前



focus

👍 1

这里有一个问题，一个chain下面有多个规则，数据包是遇到一个匹配的就执行动作，还是每个规则都去匹配呢？这里我想说都是 是否跟nginx 正则匹配那样，有优先级，每个配置都去匹配一遍？最后找到一个权重最高都规则去执行相应都动作？

2年前



DE009

👍 0

太强了！讲的十分清楚，感谢

2年前



tptpp

👍 0

第二次拜读，每次都有不一样的收货~

3年前



yichan

👍 0

真的总结的太好了，突然对于iptables豁然开朗

3年前



hanjk

👍 0

第二次拜读，讲的真通俗。

3年前



Fungit

👍 0

查找iptables发现大佬博客，前来拜读😊

3年前



Wmd

👍 0

写的很好，来点个赞

3年前



Lasnitch

👍 0

真的总结的太好了，加油！

3年前



jiftle

👍 0

感觉博主可以出专栏，写书了。
在看云上，转载了一份（前6篇）。备注了出处。
文档地址：<https://www.kancloud.cn/jiftle/iptables-detailed-introduction>
3年前



jiftle

👍 0

通俗易懂，博客用的是Hexo-theme-butterfly吧。
3年前



jojo

👍 0

文章很棒，就是想提一点建议：
1、建议多加一点例子，结合概念加深理解。
2、例子是要那种有代码和图片结果的最好。
3年前



在路上

👍 0

楼主太强了
3年前



举头望明月

👍 0

总结的清晰易懂，忍不住的非常赞
3年前



Goestu

👍 0

博主用的是wordpress博客吧，主题能分享一下嘛？谢谢
3年前



K4W1H0R53

👍 0

如果按照防火墙流量示意图的说法，流出流量是不是没法在路由选择前控制了？只能在路由选择后再进行OUTPUT>>POSTROUTING?那流出方向只用一个链不就行了，干嘛还要设置成OUTPUT+POSTROUTING？
3年前



vtrfhgbrt

👍 0

强
3年前



小白

👍 0

图片挂了。大哥

3年前



秦柏

👍 0

膜拜大佬，这是我看到的把iptables讲解的最通俗易懂的文章了

3年前



eagle711

👍 0

这是我见过写得最好的关于iptables文章了，真正理解了它的原理了，太感谢了！！

3年前



YAO

👍 0

大佬，我想在自己的一篇知乎文章中引用”数据经过防火墙的流程“下面的那张流程图，因为实在是描述的太清楚了，我会在文章中注明出处，可以吗？

3年前



朱双印 (<https://www.zsythink.net/archives/author/1>) 作者

👍 0

可以的，加油~

3年前 @YAO



阿达

👍 0

大佬太强了，iptables 总结了十几篇

3年前



Zed

👍 0

大神太牛了

3年前



zhang

👍 0

写的非常浅显易懂，终于懂了

3年前



OYXT

👍 0

说实话, 我是我见过把 iptables 四表五连解释的最清楚的文章.

3年前



阿花

👍 0

太牛了，能不能转载一下下

3年前



nazege

👍 0

写的真好！

3年前



JS

👍 0

感谢博主深入浅出的讲解,循着您的教程,写了一篇笔记性质的博客,使用了 数据经过防火墙的流程 的那张图片, 寻求授权,已经注明来源.

3年前



朱双印 (<https://www.zsythink.net/archives/author/1>) 作者

👍 2

可以的，注明来源随使用，加油

3年前 @JS



heise

👍 0

感谢博主，非精通iptables者无写出如此通俗易懂的文章。

3年前



helloworld

👍 0

这才叫深入浅出嘛，能对iptables精通后才能写出这么浅显易懂的文章！

3年前



茉茉

👍 0

豁然开朗，谢谢博主

3年前



阿帅

👍 0

可太秀了，终于找到一篇好的博客了，可以转载转载吗

3年前



sad

👍 0

虽然看不太懂 但是讲的很仔细 赞👍

3年前



carrain

👍 0

必须赞一个，概念性的东西很难写，所以很少人写，但没有概念就学操作就像浮萍，感谢
3年前



jason416

👍 0

条理清晰，感谢博主分享~
3年前



小柒的同学

👍 0

太棒了，确实很通俗易懂，感谢博主分享自己的心得，希望更多人看到。谢谢大佬！
3年前



小柒

👍 0

行文诙谐，通俗易懂，太棒了！
3年前



一个有钱的人

👍 0

辛苦！
3年前



good

👍 0

写的真好。你可以直接计算机系当教授了。
3年前



xxx

👍 0

为什么上层协议到output表之间还有个路由判断？这个路由判断的功能是做什么的？
3年前



null

👍 0

感谢博主辛勤教学！
3年前



共同学习netfilter私我，互助

👍 0

想请教博主一些问题，由于iptables自身提供的一些功能无法满足我的功能要求，请问博主有相关通过iptables接口自定义表实现相关功能的博客吗
3年前



Ruo_xiao

0

大侠，内功如此身深厚，难倒习得九阳神功？！

3年前



null

0

什么时候我才能像你一样优秀

3年前



david

0

博主，您好，您的iptables系列文章很通俗易懂。我的论文中可不可以借鉴一部分（在参考文献中以引用的形式标注）？

3年前



朱双印 (<https://www.zsythink.net/archives/author/1>) 作者

0

可以的，没问题，加油~

3年前 @david



潇潇愚歌

0

博主iptables讲解的非常好，希望能授权转载，我在下面发送了邮箱，感谢博主~~

3年前



einslssac

0

写的通俗易懂,最近也在移植iptables

3年前



迷之夏天

1

博主好，我之前也是被网上各种iptables弄晕。其实，真正的学习和思考就应该像你这样，严谨，耐心，像看一颗树一样从枝干到叶茂。这样系统的思考远比靠旷日持久的零散积累要一劳永逸的，是真正的节省时间和进步。我认为这是真正的智慧。不过，这需要你这样的大侠才能撑起来哦，往后提到iptables，我必须提到你，这就是继承吧~~谢谢啦

3年前



lion

0

内核模块 iptable_ 不带s

3年前



阿科

👍 0

通俗易懂，带有哲学，很棒！

3年前



reatang

👍 0

学习了，知识点非常的工整

3年前



吉吉馨

👍 0

讲的好清楚，学习了

3年前



冰雪树挂

👍 0

小白想问下大神，为啥我的机器里没有PREROUTING & POSTROUTING链路吗？会有影响吗？

3年前



共同学习netfilter私我，互助

👍 0

怎么可能没有呢，需要看你是什么表，filter表就没有PREROUTING,如果只是通过iptables命令行看的话，你先指定表

3年前 @冰雪树挂



alex

👍 0

有个不明白的地方，拿output 链来说，output链同时出现在raw mangle nat filter 表里，换句话说，raw mangle nat filter 这4个表都有output链，我的疑问是，这4个表引用的是完全相同的output链，还是说output链是一个大组合链= raw的output子链 + mangle的output子链 + nat的output子链 + filter的output子链？即把raw的output链的规则 + mangle的output链的规则 + nat的output链的规则 + filter的output链的规则 放在一起，组成了一个大的output规则集合

3年前



snoire

👍 0

四个表引用的是完全不同的 output 链，你的后一种理解是对的。

3年前 @alex



flytomoon

👍 1

66666写的太好了，不过我想补充一下，表的先后顺序里有逻辑，一开始我很不理解为什么raw在nat前面，查了之后才意识到raw在前面可以提高性能直接处理免得nat

3年前



@@@

👍 0

写的超赞

3年前



临江仙

👍 0

学完打个卡~~很棒

3年前



渣渣

👍 0

超级好文，通俗易懂，解答了心中所有疑惑

4年前



小兵狗二蛋

👍 0

博主你好，已经看完，写得很棒！同时有个疑问，万望回复。问题是：到底是表在链中？还是链在表中？

4年前



snoire

👍 0

表中有链，链中也有表，表和链是不同层面上的概念。表是按照功能划分，链是按照在处理流程的位置来区分的。

3年前 @小兵狗二蛋



null

👍 0

这写的，简单是良心又专业。

4年前



sky

👍 0

受教了，博主厉害，理解得很透彻，还能把自己理解的完整的表达出来，最后公开，真心佩服。

4年前



guide2it.com

👍 0

请问楼主这个网站是什么模版？

4年前



透明的灰

👍 0

看了老师写的zabbix入门，感觉找到了宝藏。简单易懂，能感觉到是位非常有耐心的人。

4年前



哈哈

👍 1

里面的比喻让知识更容易被理解

4年前



Frank

👍 0

深入浅出，通俗易懂，是真大师，十分佩服

4年前



啦啦啦

👍 0

老师，什么时候把iptables用python语言来介绍呀？

4年前



龙鲲

👍 0

从知道有防火墙这个词到现在,一直没有想过防火墙到底是怎么工作的.看了这篇文章,受益匪浅,谢谢你的分享!!!

4年前



aha

👍 0

关注了，太牛逼了通俗易懂

4年前



helloworld

👍 0

这是我看过的对iptables理解最为简单明了的一篇文章！期待后续

4年前



豌豆多多

👍 0

写的真好，通俗易懂。受益匪浅，学习了！！！！

4年前



翟码农

👍 0

写得真棒，上回看了一遍，再来加强下记忆

4年前



zhangdianpeng

👍 0

学习了

4年前



frank

👍 0

厉害厉害

4年前



chuanzang

👍 1

这个是我在网上看过的最通俗易懂的文章，一看就懂。赞！！！！！！

4年前



liunianwangfan

👍 0

小编，你的nginx恶意访问配置是怎么做的，可否讲一下，学习学习 😊 😊

4年前



朱双印 (<https://www.zsythink.net/archives/author/1>) 作者

👍 0

你跟下面的评论是一个人吧~hhhhhhhhhh~~~看来你是恶意访问了哦~~~ 😊 😊

4年前 @liunianwangfan



anyu967

👍 0

写的很好，通俗易懂。博文可以出本书啦，敢问小编从事运维多长时间了。膜拜膜拜 📱 📱 📱

4年前



wangzuo

👍 0

写的很好，请问可以转载吗？非常歇息

4年前



bin

👍 1

结合《更安全的Linux网络》一书来学习，效果更佳。

4年前



thewangcj

👍 0

通俗易懂，厉害了

4年前



小森

👍 0

博主，文章中的上层协议，都指的哪些协议呢？ip协议，以及其之上的协议吗？

4年前



你我他

0

又一个马哥学徒

4年前



遗失的美好

0

真的生动形象，好教程，支持顶一下。感谢老师，以前学前端的时候用的IDE sublime好像上面有个
人形的图标，头上的图标汉字就是朱双印，不知道是不是博主。技术大牛

4年前



朱双印 (<https://www.zsythink.net/archives/author/1>) 作者

0

呃……应该不是我……

4年前 @遗失的美好



icac

0

首先点个赞，写得很不错！文中提到【每个经过这个“关卡”的报文，都要将这条“链”上的所有规则匹
配一遍】，好像不是每条链所以规则都要匹配一遍吧，按照顺序哪条匹配到了就不再匹配该链后续
的规则了吧？

4年前



朱双印 (<https://www.zsythink.net/archives/author/1>) 作者

0

对，这句话不严谨了，后文中有提到匹配到了就不匹配的事情，准确的说，应该是，有匹配到的规
则，就按照规则执行，只有匹配不到合适规则的时候，才会都匹配一遍，以便确定最后一条规则也
不适用，不过后文中有详细的解释，所以继续向下看，没有问题的，加油~

4年前 @icac



sdsd

0

这个意思是每张表只会匹配一条规则吗？如果有多条使用的规则在同一张表里，也不会执行多条？

4年前 @朱双印



willconquer

👍 0

大牛你好。目前学习k8s中使用ipvs作为kube-proxy实现方式时，对于规则匹配有些许疑惑。主要就是集中在规则匹配。在k8s中会在nat表的prerouting chain自定义一个链，将流量jump到kube-service这条规则

```
-A PREROUTING -m comment --comment "kubernetes service portals" -j KUBE-SERVICES
```

然后在nat表中kube-service chain还会有3条规则，这里最令我疑惑的就是 如果流量是要访问service 的cluster ip那么第一个规则就能匹配，但是匹配动作是给流量打上标签。

那么打上标签之后 是不是应该继续匹配 kube-service chain中的后面的规则呢？例如第三条规则也是可以匹配的。

还有一个问题就是，我理解只有-j到accept才能跳转到下一个input 链，进而进入到filter表中的input链规则。希望可以解答！万分感谢

```
-A KUBE-SERVICES !-s 172.30.0.0/16 -m comment --comment "Kubernetes service cluster ip + port for masquerade purpose" -m set --match-set KUBE-CLUSTER-IP dst,dst -j KUBE-MARK-MASQ
```

```
-A KUBE-SERVICES -m addrtype --dst-type LOCAL -j KUBE-NODE-PORT
```

```
-A KUBE-SERVICES -m set --match-set KUBE-CLUSTER-IP dst,dst -j ACCEPT
```

4年前 @朱双印



yyc

👍 0

我有点不太明白，链的关系图中，笑脸是代表了什么呢？

4年前



yyc

👍 0

我了解了，外部服务

4年前 @yyc



朱双印 (<https://www.zsythink.net/archives/author/1>) 作者

👍 0

客户端请求

4年前 @yyc



yyc

👍 0

画的笑脸代表什么呢？在链的关系图那里

4年前



illtox

👍 0

真学到了！

4年前



czj

0

"表链关系"第一张图错了，图中nat在raw之前，实际上raw优先级更高，后面一张图是对的。

4年前



朱双印 (<https://www.zsythink.net/archives/author/1>) 作者

0

请看“注”

4年前 @czj



278080785

0

大写的佩服 谢谢老师

4年前



elliott_tijou

0

我看过最浅显易懂的iptables入门介绍了，忍不住上来给好评！

4年前



gaarahe

1

你好，请教一下。centos7 中Firewalls和iptables的status都是dead(systemctl stop firewalld和service iptables stop)，为何我iptables -L -f nat还能查询到规则，这时候的规则生效吗？

4年前



可爱小肉鸽

0

可以理解是手工直接在命令行添加的这些规则，这些规则在当前系统的“内存”中，临时生效，重启系统就没了。iptables服务的开关与否，不影响这些在内存中的临时规则。

我是这样理解的，不知道对不对~

4年前 @gaarahe



叼着辣条的猫

0

有个问题想问一下博主，困扰了好久。就是filter表与mangle表都有forward链，这有什么区别吗？博主能多给举几个例子吗？谢谢

还有就是如果/etc/sysconfig/iptables中只有filter表，那么其他表默认也全是允许通过的吗。

4年前



danding

0

个人理解，forward是一个链，这个链主要是用作转发，他对应的filter表也就是，可以在forward这个链上配置过滤规则，他和mangle表共用一条链，但是链中的规则不同而已。

4年前 @叼着辣条的猫



tafan

👍 0

写的太棒了，希望可以转载

4年前



爱吃鱼的猫

👍 0

大佬写的内容让我受益匪浅！感谢大佬！以后会一直关注的！

4年前



小菜鸟

👍 0

给大神跪了

4年前



科比

👍 0

写得真复杂，真的，零基础看了表示快速入门好难

4年前



卢哥

👍 0

写的真的非常好。

4年前



Choco Lee

👍 0

用浅显易懂的语言，描述复杂的理论，而且举例很生动形象，能很好地帮助理解

4年前



朱双印 (<https://www.zsythink.net/archives/author/1>) 作者

👍 0

尽量把我遇见的坑给填了，就不用坑你们了，加油，共勉~

4年前 @Choco Lee



duxf

👍 0

看了您的文章，感觉就像看到了一本精彩的书，真的可以出书了！

4年前



朱双印 (<https://www.zsythink.net/archives/author/1>) 作者

👍 0

能帮助到你就好，加油，共勉~

4年前 @duxf



dillan

👍 0

佩服佩服，讲的既易懂又系统

4年前



ff

👍 0

good，很好，醍醐灌顶

4年前



阿菜

👍 0

写得非常好，清晰简洁明了，特地上来感谢一下！

4年前



运维

👍 0

马哥学生？

4年前



妖冰

👍 0

表述得很清晰，我这个运维小白竟然看懂了，优秀

4年前



王飞

👍 0

我可以，用您的博客来录视频讲课嘛

4年前



朱双印 (<https://www.zsythink.net/archives/author/1>) 作者

👍 0

可以的，说明一下就行的~

4年前 @王飞



小白

👍 0

啥时讲讲openldap相关的知识

4年前 @朱双印



z5wjz

👍 0

看过的最好的表述

4年前



reid

👍 0

大神级，无论是知识还是逻辑都讲的很清楚。

4年前



又摘桃花换酒钱0

👍 0

博主，写的真心不错啊

4年前



光头小子

👍 0

非常详细，感谢，终于入门了。

4年前



time

👍 0

66666! 博主写的真好

4年前



William

👍 0

感谢

4年前



xiaoxin008

👍 0

浅显易懂 不错!

4年前



chen

👍 0

写得深入浅出、形象生动、易于理解，非常感谢

4年前



布哈林

👍 0

非常感谢

4年前



fanmingyi

👍 0

是我见过最好的文献 非常感谢

4年前



小明明

👍 0

讲的很好

4年前



MedusaSTears

👍 0

有幸并荣幸看到这篇文章,对我一个刚接触iptables的人来说,由浅入深,循序渐进的学习,包括经典的那个图的整理,真是费心了,非常感谢

4年前



JR

👍 0

太棒了!!!加油!!!

4年前



fly

👍 0

写得非常好,谢谢博主

4年前



ddd

👍 1

谷歌下packet flow in netfilter and general networking这张图片,这包含了iptables在各种场景的处理流程。建议放到网页中更清晰

4年前



cp

👍 0

非常好理解的文章。赞

4年前



深奥

👍 0

非常好,真是好东西

4年前



杰儿

👍 0

非常好呢! 赞赞赞

5年前



杰儿

👍 0

如何转载呢! 谢谢

5年前



ZKeeer

👍 0

博主的iptables系列文章给了我很大的帮主，感谢~
希望能允许转载这篇文章到我自己的博客，会著名作者和出处，本系列其他文章用链接的形式给出来。

5年前



然然

👍 0

这个前端用的什么框架啊？

5年前



老张

👍 0

支持 iptables 系列出书，绝对精品。

5年前



毛毛

👍 0

厉害，关键是白话解释，易懂。可能会摘抄一点写笔记哈~

5年前



Kane Zheng

👍 0

给小白以浅显易懂的方式讲明白才是真高手，膜拜！

5年前



Moab、

👍 0

目前见过最好的博客之一

5年前



摩王

👍 0

真是个人才啊。

5年前



长勋

👍 0

你好，请问图中forward 阶段之后为啥还需要一次路由过程？

5年前



sszzw

👍 0

这里明显写错了。。

5年前 @长勋

之前的评论里面有讨论这个问题，参考了一些资料，有这个路由判断，但是如果按照wiki中的图片来说，准确的来说不应该放在forward与output交接处，而应该放在output的中间位置，如此图所示 <https://en.wikipedia.org/wiki/Netfilter#/media/File:Netfilter-packet-flow.svg> (<https://en.wikipedia.org/wiki/Netfilter#/media/File:Netfilter-packet-flow.svg>) 但是按照之前某资料的参考，连接是<http://www.iptables.info/en/structure-of-iptables.html>（这个网站现在打不开了，在之前讨论时，可以看到其中的路由判断的图），这个具体是什么样的我再确定一下，可以先待定或者我把图上的先去掉

5年前 @sszzw



Yoao

👍 0

朱哥 您可以写本书了 贼详细 贼好

5年前



laogou

👍 0

大哥推荐来看的，先赞再看！

5年前



小土豆

👍 0

赞 一下就懂了

5年前



JAY

👍 0

写得真的很通俗易懂，一下就看懂了。链表那里讲得很清晰，一下子就形成概念了，感觉很多文章只讲原理，又不解释为啥么这么做。

5年前



helloworld

👍 0

厉害~

5年前



贝克

👍 0

作者写的真是太好了。比喻，图表，简直让人看得舒畅！

5年前



毛也择西

👍 0

平心而论，特么写的真好，慢慢学习中。

5年前



hustpigeon

👍 0

很喜欢你的文章，全都讲到核心了。厉害

5年前



pocket knives europe

👍 0

Thanks for finally talking about >iptables详解：图文并茂理解iptables <Liked it!

5年前



山海经

👍 0

写的很棒，通俗易懂，谢谢博主分享~

5年前



阿森纳枪王

👍 0

请问是否可以转载，我会注明出处，另外我有一个个人技术分享网站www.kaonao.net，是否可以互换友链，我刚做不久，但正在逐步丰富

5年前



臣

👍 0

是我至今位置找到的最适合小白看的文章，谢谢

5年前 @阿森纳枪王



CZH

👍 0

初来乍到，先留个言再好好学习学习 😊

5年前



an anonymous adorer

👍 0

向博主致敬，感谢您的无私分享~

5年前



bury

👍 0

写的太好了。简直是是要不要的了。目前也是正在学习运维路上的苦逼大学生。弱弱问一句您，可以转载您的文章吗

5年前



O记

👍 0

朱先生，可不可以手动转载？

5年前



route2h

👍 0

感谢博主，iptables概念写的很好，收藏了

5年前



songrgg

👍 0

写的真好，以简单的方式将这个不算简单的问题讲清楚了，棒！

5年前



xiaobai

👍 0

感谢博主，终于搞明白了，写的太好了，我要推荐给其他同事看看，博主牛牛牛!

5年前



sonyta

👍 0

写的真不错，形象直观

5年前



雨后龙井

👍 0

写得非常好，清晰、明了。

5年前



add

👍 0

你好啊 关于先路由还是先走output链，netfilter维基百科里的第二个图，有画出是先决定路由再走output链的，其二我觉得output链中可以通过-o参数过滤出网卡，这也是需要先进行路由判断才能知道数据包要从哪块网卡出去吧，wiki链接：<https://en.wikipedia.org/wiki/Netfilter>

5年前



朱双印 (<https://www.zsythink.net/archives/author/1>) 作者

👍 0

感谢客官提供了具体的连接，解决了我一直疑惑拿不准的地方，图片已经修改，@add 谢谢还有也谢谢 @nick，也提出了问题所在，只是当时没有参考我就没有修改 @add 学习了，感谢，有空常来捧场~

5年前 @add



pengpeng

👍 0

写的条例非常清晰，对于刚开始接触iptables 都非常容易理解。

5年前



kaiw

👍 0

写得很好，连我这个之前从来没有了解过防火墙，netfilter的人都能看懂，一定花了很多时间。语句生动易懂，配图也非常容易理解。非常感谢。

5年前



思绪飘然

👍 0

写得太棒了！

5年前



meng

👍 0

写的非常棒，已收藏；

5年前



lirics

👍 0

微信6元，绵薄之意

5年前



11

👍 0

写得太好了，网上其他的文章都不容易懂，这篇文章很容易让人理解

5年前



feng

👍 0

建议贵站不要禁用左右键

5年前



wax5798

👍 0

博主，您好，能否授权我转载此篇文章呢

5年前



nick

👍 0

文章写的很好，通俗易懂，不过有张图应该画的有点问题
数据包发送流程中OUTPUT之前应该有一个路由判断点

5年前



朱双印 (<https://www.zsythink.net/archives/author/1>) 作者

👍 0

这个路由判断点我也一直有疑问，之前也是认为是在OUTPUT之前的，因为参考了很多文档，大多数都是在OUTPUT之后，所以没有找到确切的官方文献之前就参考了大多数人的图

5年前 @nick



菜鸟

👍 0

言简意赅，深入浅出 😊

5年前



梧桐树

👍 0

通俗易懂，非常棒！！

5年前



rufengsuixing

👍 0

发现不能复制和右键之后，换成了谷歌浏览器按下了f12 😊

哇，大开眼界，几行js就能屏蔽掉右键和拖拽

讲的很好，受教了

点赞收藏加支持

5年前



新之助

👍 0

感谢博主啊，在网上找了好多资料，只有你这里说的最清楚，这些基本概念讲的非常清楚

5年前



kl

👍 0

通俗易懂！受教了

5年前



suveng

👍 0

最近在看Linux的书，看到防火墙，大概的了解，还是有点蒙，现在看完大佬的，强无敌。
另外》》我也想搭一个不能复制的博客，求指点。

5年前



朱双印 (<https://www.zsythink.net/archives/author/1>) 作者

👍 0

wp插件CopyrightPro

5年前 @suveng



dyf

👍 0

超赞一个，若干讲iptables的资料看完后是若干的疑惑，唯有此文醍醐灌顶！能把这一概念讲得如此清晰，博主功力了得呀

5年前 @朱双印



Jeff

👍 0

看了一下arch Linux官网iptables一章，不知所云。看了你的博客，恍然大悟，深入浅出，写得太好了！

5年前



斗心魔者

👍 0

请问博主的站点用的什么框架？是开源还是自己写的哟？

6年前



flyzy2005

👍 0

你好博主，转载应该怎么声明？

6年前



flyzy2005

👍 0

博主你好，我想转载你的iptables系列1 2 3，可以吗？保留出处~

6年前 @flyzy2005



net_czc

👍 0

看完mysql系列，再看iptables系列；iptables的概念说的引用现在流行的一句话：接地气，显浅易懂；构思和码字耗费了不少功夫，留意支持一个 🍻

6年前



xinli

👍 0

跟着您的博文学习，希望能够转载，转载保留出处，谢谢您！

6年前



卡卡Bin

👍 0

文章内容讲解很透彻，通俗易懂，感谢分享，能否发一份到我邮箱呢，谢谢！之前邮箱写错了 重新修改了下

6年前



落叶随风

👍 0

您好，请教一下，Netfilter的Hook函数 与 Iptables的规则是什么关系呢？

6年前



朱双印 (<https://www.zsythink.net/archives/author/1>) 作者

👍 0

Netfilter是框架，iptables是客户端工具，通过iptables设置规则

6年前 @落叶随风



共同学习netfilter私我，互助

👍 0

你写的iptables规则，实质性在内核里的操作就是通过注册hook函数，来实现数据包的过滤等等功能

3年前 @落叶随风



籽籽

👍 0

数据流经防火墙的流程这个图，为什么FORWARD后面还有一个路由判断，疑问？

6年前



朱双印 (<https://www.zsythink.net/archives/author/1>) 作者

👍 0

参考了一些资料，发现大多数资料的流程中都包含这个路由判断，可以参考如下文章的中流程图
<http://www.iptables.info/en/structure-of-iptables.html> (<http://www.iptables.info/en/structure-of-iptables.html>)

具体原因没搞明白，搞明白了告诉我

6年前 @籽籽



Ray

👍 0

是不是要考虑下有多个出口的情况呢,要判断从哪个接口出去呢

5年前 @籽籽



tmswd

👍 0

这个路由判断是判断把数据包从哪个接口发出去 用ip route可以查看路由表 上面带有接口信息

5年前 @籽籽



至夏

👍 0

进来的数据包的目的有可能是本地 也有可能是其它网络中的主机,所以需要一次路由判断,是本地的就直接交本地协议栈了,否则进行转发.另一个路由是对本地产生的数据包进行一次目的判断,不然怎么知道数据包要从哪个接口出去呢,,但有个问题: 这里的路由判断是在OUTPUT链处理之前呢还是之后,如果在之前,就像图中的那样,那OUTPUT链上的DNAT规则岂不是废了,如果路由在OUPUT链后面,那在链上处理时数据包可能还没有确定源地址呢..

5年前 @籽籽



TONY

0

请教一下，我单网卡双IP，IP1为192.168.15.3/24,网关192.168.15.1，解析DNS：192.168.15.1，IP2为：30.16.204.15/22网关30.16.204.1,解析DNS为30.0.0.16.我现在想本机所有30.0.0.0网段的访问请求，都走IP2对应的网关，并且由IP2的DNS负责解析；其他的非30.0.0.0网段的请求，全部走IP1网关，并有IP1对应的DNS负责解析。用iptables可以实现我的要求吗？

6年前



Ray

0

网关即为默认路由，如果指定两个网关，目的数据包该匹配哪个网关呢？写明细路由

5年前 @TONY



三个石头

0

大佬，我想把iptables相关的资料转载到或者做成PDF保存下

6年前



问天

0

朱兄：

我配置的iptables规则如下 <http://www.bladeblue.top/wp-content/uploads/2017/08/iptables.txt>

我新配置的规则 在nat 表中的 IPMAP 和IPMAP链中的两条规则如下

```
-A IPMAP -d 10.0.2.2/32 -m iprange--src-range 10.0.2.176-10.0.2.176 -j DNAT --to-destination 127.1.0.61
```

```
-A IPMAPNAT -d 127.1.0.61/32 -m iprange--src-range 10.0.2.176-10.0.2.176 -j SNAT --to-source 127.1.0.2
```

IPMAP引用在nat表中的PREROUTING链中 IPMAPNAT 引用在 POSTROUTING链中

操作的时候 数据从10.0.2.176终端发送到 10.0.2.2上 最后在127.1.0.61上接收到了 127.1.0.2发来的数据

但是我配置的这两条规则 在通过 iptables -t nat -nvl 查看的时候 前面的计数 和流量并没有变化 向前看 看raw的 PREROUTING 和mangle的PREROUTING却有变化，不知道为什么？烦请朱兄指点一二..

6年前



jiangshan

0

智障的我竟然看懂啦 稳稳稳

6年前



朱双印 (<https://www.zsythink.net/archives/author/1>) 作者

0

客官自黑捧场更稳，常来呦~~

6年前 @jiangshan



bluse

👍 0

印大博主，能讲讲ipfw么？

6年前



KeithK

👍 0

很详细哦哦哦！博主文章都学习性真高！加油！

6年前



朱双印 (<https://www.zsythink.net/archives/author/1>) 作者

👍 0

能帮助到你就好哦~

6年前 @KeithK



白衣 年代

👍 0

写得真好。

6年前



it小菜鸟

👍 0

以后就跟你学习咯

6年前



朱双印 (<https://www.zsythink.net/archives/author/1>) 作者

👍 0

共同努力，共同进步~加油~~

6年前 @it小菜鸟



haha

👍 0

博主写的真好的呀！

6年前



chinenglish

👍 0

感谢博主，非常赞，讲解iptables最好的文章

6年前



卧石青篱

👍 0

运气不错，最近想了解下iptables和netfilter，刚好发现了博主的文章 😊

6年前

 **朱双印** (<https://www.zsythink.net/archives/author/1>) 作者

👍 0

能帮助到客官就是最好的 😊

6年前 @卧石青篱



蓝翔博士后

👍 0

感谢博主，非常清晰明了，点赞！

6年前



叫我大宝酱

👍 0

666666 赞赞赞 厉害了我的哥

6年前



时光

👍 0

非常详细。感谢分享

6年前



时光

👍 0

非常详细，明了。谢谢

6年前

 **朱双印** (<https://www.zsythink.net/archives/author/1>) 作者

👍 0

客官的肯定是我前进的动力，谢谢支持~

6年前 @时光



max linux

👍 0

能否也发我邮箱一份，谢谢啦~

6年前



fyczy

👍 0

非常感谢楼主分享，我正在学习这块知识，能否发我邮箱一份，谢谢

6年前



斷點

👍 0

很棒啊，醍醐灌顶

6年前

 **朱双印** (<https://www.zsythink.net/archives/author/1>) 作者

👍 0

能帮到你就好，常来捧场哟

6年前 @斷點



fanren224

👍 0

博主写的很好，可以转载到我的博客吗

6年前



傻瓜

👍 0

学习了，谢谢博主无私分享！

6年前



bluse

👍 0

这样的文章很能提高读者的学习效率。

感谢双印的辛勤付出！

6年前

 **朱双印** (<https://www.zsythink.net/archives/author/1>) 作者

👍 0

感谢兄弟的评价，有你的支持，写博客动力变足了，加油~

6年前 @bluse



maxie

👍 0

您好，您写的文章真的不错，学习了。可以转载到我的博客吗？

6年前



maxie

👍 0

mcy19950930@gmail.com

谢谢啦~~~~

6年前 @maxie



nanu

👍 0

透彻

6年前



youlinux

👍 0

很吊 呵呵

6年前

 **朱双印** (<https://www.zsythink.net/archives/author/1>) 作者

👍 0

哈哈，习杰，捧场来了，谢谢啦兄弟 😊

6年前 @youlinux



Forz

👍 0

博主这篇博文是我见过的同类文章中最好的！求转载！

6年前



echo

👍 0

送博主三个字 写的太吊了

6年前

 **朱双印** (<https://www.zsythink.net/archives/author/1>) 作者

👍 0

从你的评论能够感觉到客官绝非等闲之辈，日后必成大器~~~~

6年前 @echo



请输入您的QQ号

👍 0

```
[root@localhost sysconfig]# iptables -L
```

```
Chain INPUT (policy ACCEPT)
```

target	prot	opt	source	destination	state
ACCEPT	all	--	anywhere	anywhere	RELATED,ESTABLISHED

ACCEPT	icmp	--	anywhere	anywhere	
--------	------	----	----------	----------	--

ACCEPT	all	--	anywhere	anywhere	
--------	-----	----	----------	----------	--

ACCEPT	tcp	--	anywhere	anywhere	state NEW tcp dpt:ssh
--------	-----	----	----------	----------	-----------------------

REJECT	all	--	anywhere	anywhere	reject-with icmp-host-prohibited
--------	-----	----	----------	----------	----------------------------------

请问 REJECT all -- anywhere anywhere reject-with icmp-host-prohibited 这句话是什么意思？

我远程linux的桌面时，必须关闭防火墙吗？可以不关闭 怎么配置呢？求指教

6年前

 **朱双印** (<https://www.zsythink.net/archives/author/1>) 作者

👍 0

最后一句话的意思就是拒绝所有包，这样配置表示使用白名单机制

如果你不明白为什么这样配置，可以看完本博客中的IPTables系列文章，系列文章地址如下

iptables零基础入门系列 (<https://www.zsythink.net/archives/tag/iptables/>)

直到如下文章

iptables的黑白名单机制 (<https://www.zsythink.net/archives/1604>)

你所贴出的示例在博客中有解释，你的问题在博客中也有相应的答案，耐心看完系列文章即可明白，谢谢关注

6年前 @请输入您的QQ号



小凡

👍 0

写得真好，已经收藏并关注，感谢辛苦写作！

6年前



朱双印 (<https://www.zsythink.net/archives/author/1>) 作者

👍 0

😊 已经在微信公众平台中看到了你的关注

6年前 @小凡



静心学习

👍 0

感谢博主的分享，希望可以转载到自己的博客

6年前



丁一

👍 0

你好，iptables的内容写的真好，我之前看了那么多，还是这个写的详细又清晰，也申请转载到个人博客，以便更多人学习，非常感谢！

6年前 @静心学习



朱双印 (<https://www.zsythink.net/archives/author/1>) 作者

👍 0

转载授权已发送至邮箱：dXXXXXXXXXi@qq.com 请查收。

6年前 @丁一



二哥

👍 1

我就喜欢这种评论的样式一层套一层，可以一直套下去

4年前 @朱双印



humour

👍 0

写的好

4年前 @二哥



mapix

👍 0

楼主写的很易懂，赞一个。有个小问题没理解，如果定义在 nat 表中的规则列表会在 prerouting, postrouting, input, output 链上生效，那在这四个链上做匹配的时候都是用的同一堆规则么。比如加 rule1 到 nat 表，那这个 rule1 会同时在这四个路径上生效？也就是说，nat 表只有一个，所以加入的规则都会在各种阶段同时生效？

6年前

哦,看了下在第二篇文章有说! 是独立的.

6年前 @mapix



一本杂书

👍 0

写的非常好，通俗易懂。。如何能转载呢，可以吗

6年前



朱双印 (<https://www.zsythink.net/archives/author/1>) 作者

👍 0

转载授权已经发送到：XXXX5@qq.com，谢谢关注。

6年前 @一本杂书



了尘

👍 0

写的不错，可以授权转载吗？

6年前



千叶归来

👍 0

不错 直白 明了

6年前



烟波鱼籽

👍 0

看到的关于iptables解说最为深入浅出的一篇，给您大大的赞！楼主功力深厚啊！

6年前



朱双印 (<https://www.zsythink.net/archives/author/1>) 作者

👍 0

客官很有眼光啊~我就喜欢你这种敢于说实话的人~嘿嘿~

6年前 @烟波鱼籽



呵呵哒

👍 1

写的不错。能用直白简单的类比来解释计算机的知识，是能力的体现。

6年前



SecurityMap

👍 1

您好，您的这篇文档写的非常棒，希望转载，请授权，谢谢！

6年前



👍 1

在您的站上没有看到联系方式，方便给个 email 吗？

6年前 @SecurityMap



👍 1

谢谢你的关注，关于本博客的沟通，可通过邮箱 zsythink@yeah.net 进行

6年前 @SecurityMap