转载 iptables基础知识详解

2018-09-13 11:41:24 LarryHai6 阅读数 9619 更多

iptables防火墙可以用于创建过滤(filter)与NAT规则。所有Linux发行版都能使用iptables，因此理解如何配置 iptables将会帮助你更有效地管理Linux防火墙。如
接触iptables，你会觉得它很复杂，但是一旦你理解iptables的工 作原理，你会发现其实它很简单。

首先介绍iptables的结构：iptables -> Tables -> Chains -> Rules. 简单地讲，tables由chains组成，而chains又由rules组成。如下图所示。

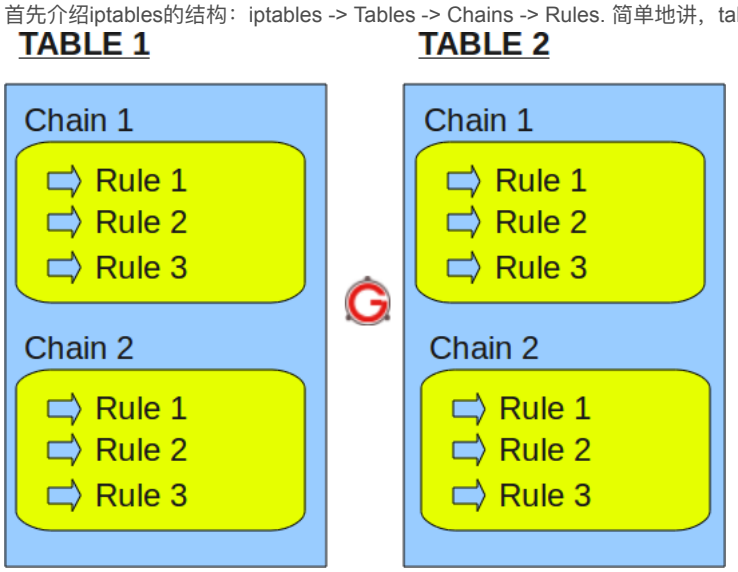


图: IPTables Table, Chain, and Rule Structure

一、iptables的表与链

iptables具有Filter, NAT, Mangle, Raw四种内建表：

1. Filter表

Filter表示iptables的默认表，因此如果你没有自定义表，那么就默认使用filter表，它具有以下三种内建链：

- **INPUT链** – 处理来自外部的数据。
- **OUTPUT链** – 处理向外发送的数据。
- **FORWARD链** – 将数据转发到本机的其他网卡设备上。

2. NAT表

NAT表有三种内建链：

- **PREROUTING链** – 处理刚到达本机并在路由转发前的数据包。它会转换数据包中的目标IP地址（destination ip address），通常用于DNAT(destination
- **POSTROUTING链** – 处理即将离开本机的数据包。它会转换数据包中的源IP地址（source ip address），通常用于SNAT（source NAT）。
- **OUTPUT链** – 处理本机产生的数据包。

3. Mangle表

Mangle表用于指定如何处理数据包。它能改变TCP头中的QoS位。Mangle表具有5个内建链：

- PREROUTING
- OUTPUT
- FORWARD

- INPUT
- POSTROUTING

4. Raw表

Raw表用于处理异常，它具有2个内建链：

- PREROUTING chain
- OUTPUT chain

5.小结

下图展示了iptables的三个内建表：

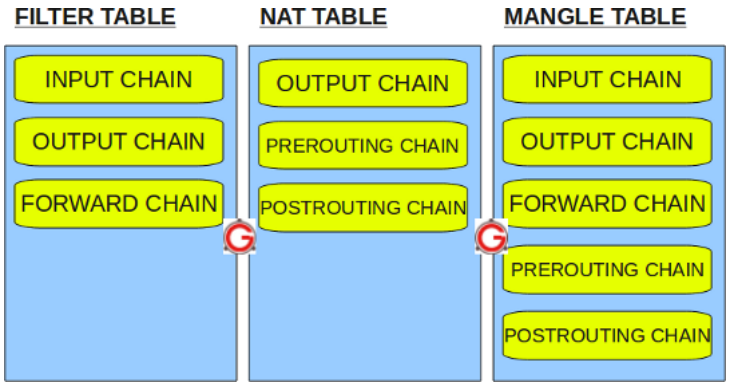


图: IPTables 内建表

二、IPTABLES 规则(Rules)

牢记以下三点式理解iptables规则的关键：

- Rules包括一个条件和一个目标(target)
- 如果满足条件，就执行目标(target)中的规则或者特定值。
- 如果不满足条件，就判断下一条Rules。

目标值（Target Values）

下面是你可以在target里指定的特殊值：

- **ACCEPT** – 允许防火墙接收数据包
- **DROP** – 防火墙丢弃包
- **QUEUE** – 防火墙将数据包移交到用户空间
- **RETURN** – 防火墙停止执行当前链中的后续Rules，并返回到调用链(the calling chain)中。

如果你执行iptables –list你将看到防火墙上的可用规则。下例说明当前系统没有定义防火墙，你可以看到，它显示了默认的filter表，以及表内默认的input链, f
output链。

```
# iptables -t filter –list
Chain INPUT (policy ACCEPT)
target    prot opt source               destination

Chain FORWARD (policy ACCEPT)
target    prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target    prot opt source               destination
```

查看mangle表：

iptables -t mangle –list

查看NAT表：

iptables -t nat –list

查看RAW表：

iptables -t raw –list

!注意：如果不指定 **-t**选项，就只会显示默认的 **filter**表。因此，以下两种命令形式是一个意思：

iptables -t filter –list
(or)
iptables –list

以下例子表明在filter表的input链, forward链, output链中存在规则：

```
# iptables –list
Chain INPUT (policy ACCEPT)
num       target                prot    opt       source          destination
1    RH-Firewall-1-INPUT     all      —         0.0.0.0/0         0.0.0.0/0

Chain FORWARD (policy ACCEPT)
num       target                prot    opt       source          destination
1      RH-Firewall-1-INPUT   all       –      0.0.0.0/0          0.0.0.0/0

Chain OUTPUT (policy ACCEPT)
num  target    prot opt source              destination

Chain RH-Firewall-1-INPUT (2 references)
num  target    prot opt source              destination
1    ACCEPT    all  –  0.0.0.0/0           0.0.0.0/0
2    ACCEPT    icmp –  0.0.0.0/0            0.0.0.0/0         icmp type 255
3    ACCEPT    esp  –  0.0.0.0/0           0.0.0.0/0
4    ACCEPT    ah   –  0.0.0.0/0           0.0.0.0/0
5    ACCEPT    udp  –  0.0.0.0/0           224.0.0.251       udp dpt:5353
6    ACCEPT    udp  –  0.0.0.0/0           0.0.0.0/0         udp dpt:631
7    ACCEPT    tcp  –  0.0.0.0/0           0.0.0.0/0         tcp dpt:631
8    ACCEPT    all  –  0.0.0.0/0           0.0.0.0/0         state RELATED,ESTABLISHED
9    ACCEPT    tcp  –  0.0.0.0/0           0.0.0.0/0         state NEW tcp dpt:22
10   REJECT    all  –  0.0.0.0/0           0.0.0.0/0         reject-with icmp-host-prohibited
```

以上输出包含下列字段：

- num – 指定链中的规则编号
  target – 前面提到的target的特殊值
  prot – 协议：tcp, udp, icmp等
  source – 数据包的源IP地址
  destination – 数据包的目标IP地址

三、清空所有iptables规则

在配置iptables之前，你通常需要用iptables –list命令或者iptables-save命令查看有无现存规则，因为有时需要删除现有的iptables规则：

```
iptables –flush
或者
iptables -F
```

这两条命令是等效的。但是并非执行后就万事大吉了。你仍然需要检查规则是不是真的清空了，因为有的linux发行版上这个命令不会清除NAT表中的规则，↓除：

```
iptables -t NAT -F
```

四、永久生效

当你删除、添加规则后，这些更改并不能永久生效，这些规则很有可能在系统重启后恢复原样。为了让配置永久生效，根据平台的不同，具体操作也不同。下绍：

1.Ubuntu

首先，保存现有的规则：

iptables-save > /etc/iptables.rules

然后新建一个bash脚本，并保存到 */etc/network/if-pre-up.d/*目录下：

```
#!/bin/bash
iptables-restore < /etc/iptables.rules
```

这样，每次系统重启后iptables规则都会被自动加载。

！注意：不要尝试在.bashrc或者.profile中执行以上命令，因为用户通常不是root，而且这只能在登录时加载iptables规则。

2.CentOS, RedHat

```
# 保存iptables规则
service iptables save

# 重启iptables服务
service iptables stop
service iptables start
```

查看当前规则：

cat /etc/sysconfig/iptables

五、追加iptables规则

可以使用iptables -A命令追加新规则，其中 **-A**表示 **Append**。因此， **新的规则将追加到链尾。**

一般而言，最后一条规则用于丢弃(DROP)所有数据包。如果你已经有这样的规则了，并且使用 **-A**参数添加新规则，那么就是无用功。

1.语法

iptables -A chain firewall-rule

- -A chain – 指定要追加规则的链
- firewall-rule – 具体的规则参数

2.描述规则的基本参数

以下这些规则参数用于描述数据包的协议、源地址、目的地址、允许经过的网络接口，以及如何处理这些数据包。这些描述是对规则的基本描述。

-p 协议（protocol）

- 指定规则的协议，如tcp, udp, icmp等，可以使用**all**来指定所有协议。
- 如果不指定**-p**参数，则默认是**all**值。这并不明智，请总是明确指定协议名称。
- 可以使用协议名(如tcp)，或者是协议值（比如6代表tcp）来指定协议。映射关系请查看*/etc/protocols*
- 还可以使用**–protocol**参数代替**-p**参数

-s 源地址（source）

- 指定数据包的源地址
- 参数可以使IP地址、网络地址、主机名
- 例如：-s 192.168.1.101指定IP地址
- 例如：-s 192.168.1.10/24指定网络地址

- 如果不指定-s参数，就代表所有地址
- 还可以使用**–src**或者**–source**

-d 目的地址（destination）

-j

数据包

ETURN，MASQUERADE

snat中的一种特例，可以实现自动化的snat（详情见上一篇文章）。

-i

, PREROUTE链

的数据包

接口的数据包

eth0以外的接口进入的数据包

th开头的接口进入的数据包

-o

UT, POSTROUTING链

接口都可以作为输出接口

接口输出

接口输出

3.

对 还希望指定端口、TCP标志、ICMP类型等内容。

–s 或者 -p udp

port 22″与”–sport ssh”。

22:100″

–p tcp 或者 -p udp

-tcp-flags TCP 标志 针对-p tcp

RG, PSH

4.

本 地计算机，其他一切连接（包括ping）都将被拒绝。

清空所有iptables规则

ip

ACCEPT

ip

ip

六

上 要发送出去的数据包却没有任何限制。本节主要介绍如何更改链策略，以改变链的行为。

1.

/!\ 上测试！

当我们使用-L选项验证当前规则是发现 所有的链旁边都有 **policy ACCEPT**标注，这表明当前链的默认策略为ACCEPT：

C

ta

A e tcp dpt:ssh

D

C

ta

Chain OUTPUT (policy ACCEPT)

ta

这 那么默认情况下将采用ACCEPT策略进行过滤。除非：

a)

ip

ip

ip

b)

ip

ip

ip

 了iptables，并且现在使用的是SSH进行连接的，那么会话恐怕已经被迫终止了！

为什么呢？因为我们已经把OUTPUT链策略更改为DROP了。此时虽然服务器能接收数据，但是无法发送数据：

```
# iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  –  anywhere             anywhere            tcp dpt:ssh
DROP       all  –  anywhere             anywhere

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy DROP)
target     prot opt source               destination
```

七、配置应用程序规则

尽管5.4节已经介绍了如何初步限制除SSH以外的其他连接，但是那是在链默认策略为ACCEPT的情况下实现的，并且没有对输出数据包进行限 制。本节在以SSH和HTTP所使用的端口为例，教大家如何在默认链策略为DROP的情况下，进行防火墙设置。在这里，我们将引进一种新的 参数-m state，并检查数据段。

1.SSH

```
# 1.允许接收远程主机的SSH请求
iptables -A INPUT -i eth0 -p tcp –dport 22 -m state –state NEW,ESTABLISHED -j ACCEPT

# 2.允许发送本地主机的SSH响应
iptables -A OUTPUT -o eth0 -p tcp –sport 22 -m state –state ESTABLISHED -j ACCEPT
```

- **-m state:** 启用状态匹配模块（state matching module）
- **–-state:** 状态匹配模块的参数。当SSH客户端第一个数据包到达服务器时，状态字段为NEW；建立连接后数据包的状态字段都是ESTABLISHED
- **–sport 22:** sshd监听22端口，同时也通过该端口和客户端建立连接、传送数据。因此对于SSH服务器而言，源端口就是22
- **–dport 22:** ssh客户端程序可以从本机的随机端口与SSH服务器的22端口建立连接。因此对于SSH客户端而言，目的端口就是22

如果服务器也需要使用SSH连接其他远程主机，则还需要增加以下配置：

```
# 1.送出的数据包目的端口为22
iptables -A OUTPUT -o eth0 -p tcp –dport 22 -m state –state NEW,ESTABLISHED -j ACCEPT

# 2.接收的数据包源端口为22
iptables -A INPUT -i eth0 -p tcp –sport 22 -m state –state ESTABLISHED -j ACCEPT
```

2.HTTP

HTTP的配置与SSH类似：

```
# 1.允许接收远程主机的HTTP请求
iptables -A INPUT -i eth0 -p tcp –dport 80 -m state –state NEW,ESTABLISHED -j ACCEPT

# 1.允许发送本地主机的HTTP响应
iptables -A OUTPUT -o eth0 -p tcp –sport 80 -m state –state ESTABLISHED -j ACCEPT
```

3.完整的配置

```
# 1.删除现有规则
iptables -F

# 2.配置默认链策略
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT DROP
```

3.允许远程主机进行SSH连接
iptables -A INPUT -i eth0 -p tcp –dport 22 -m state –state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp –sport 22 -m state –state ESTABLISHED -j ACCEPT

4.允许本地主机进行SSH连接
iptables -A OUTPUT -o eth0 -p tcp –dport 22 -m state –state NEW,ESTABLISHED -j ACCEPT
iptables -A INPUT -i eth0 -p tcp –sport 22 -m state –state ESTABLISHED -j ACCEPT

5.允许HTTP请求
iptables -A INPUT -i eth0 -p tcp –dport 80 -m state –state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp –sport 80 -m state –state ESTABLISHED -j ACCEPT

iptables命令是Linux上常用的防火墙软件，是netfilter项目的一部分。可以直接配置，也可以通过许多前端和图形界面配置。

语法

```
iptables(选项)(参数)
```

选项

```
-t<表>：指定要操纵的表；
-A：向规则链中添加条目；
-D：从规则链中删除条目；
-i：向规则链中插入条目；
-R：替换规则链中的条目；
-L：显示规则链中已有的条目；
-F：清楚规则链中已有的条目；
-Z：清空规则链中的数据包计算器和字节计数器；
-N：创建新的用户自定义规则链；
-P：定义规则链中的默认目标；
-h：显示帮助信息；
-p：指定要匹配的数据包协议类型；
-s：指定要匹配的数据包源ip地址；
-j<目标>：指定要跳转的目标；
-i<网络接口>：指定数据包进入本机的网络接口；
-o<网络接口>：指定数据包要离开本机所使用的网络接口。
```

iptables命令选项输入顺序：

```
iptables -t 表名 <-A/I/D/R> 规则链名 [规则号] <-i/o 网卡名> -p 协议名 <-s 源IP/源子网> --sport 源端口 <-d 目标IP/目标子网> --dport 目标端口
```

表名包括：

- **raw**：高级功能，如：网址过滤。
- **mangle**：数据包修改（QOS），用于实现服务质量。
- **net**：地址转换，用于网关路由器。
- **filter**：包过滤，用于防火墙规则。

规则链名包括：

- **INPUT链**：处理输入数据包。
- **OUTPUT链**：处理输出数据包。
- **PORWARD链**：处理转发数据包。
- **PREROUTING链**：用于目标地址转换（DNAT）。
- **POSTOUTING链**：用于源地址转换（SNAT）。

动作包括：

- **accept**：接收数据包。

- **DROP**：丢弃数据包。
- **REDIRECT**：重定向、映射、透明代理。
- **SNAT**：源地址转换。
- **DNAT**：目标地址转换。
- **MASQUERADE**：IP伪装（NAT），用于ADSL。
- **LOG**：日志记录。

实例

清除已有iptables规则

```
iptables -F
iptables -X
iptables -Z
```

开放指定的端口

```
iptables -A INPUT -s 127.0.0.1 -d 127.0.0.1 -j ACCEPT               #允许本地回环接口(即运行本机访问本机)
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT    #允许已建立的或相关连的通行
iptables -A OUTPUT -j ACCEPT         #允许所有本机向外的访问
iptables -A INPUT -p tcp --dport 22 -j ACCEPT    #允许访问22端口
iptables -A INPUT -p tcp --dport 80 -j ACCEPT    #允许访问80端口
iptables -A INPUT -p tcp --dport 21 -j ACCEPT    #允许ftp服务的21端口
iptables -A INPUT -p tcp --dport 20 -j ACCEPT    #允许FTP服务的20端口
iptables -A INPUT -j reject       #禁止其他未允许的规则访问
iptables -A FORWARD -j REJECT     #禁止其他未允许的规则访问
```

屏蔽IP

```
iptables -I INPUT -s 123.45.6.7 -j DROP       #屏蔽单个IP的命令
iptables -I INPUT -s 123.0.0.0/8 -j DROP      #封整个段即从123.0.0.1到123.255.255.254的命令
iptables -I INPUT -s 124.45.0.0/16 -j DROP    #封IP段即从123.45.0.1到123.45.255.254的命令
iptables -I INPUT -s 123.45.6.0/24 -j DROP    #封IP段即从123.45.6.1到123.45.6.254的命令是
```

查看已添加的iptables规则

```
iptables -L -n -v
Chain INPUT (policy DROP 48106 packets, 2690K bytes)
 pkts bytes target     prot opt in     out     source               destination
 5075  589K ACCEPT     all  --  lo     *       0.0.0.0/0            0.0.0.0/0
 191K   90M ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22
1499K  133M ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:80
4364K 6351M ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
 6256  327K ACCEPT     icmp --  *      *       0.0.0.0/0            0.0.0.0/0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 3382K packets, 1819M bytes)
 pkts bytes target     prot opt in     out     source               destination
 5075  589K ACCEPT     all  --  *      lo      0.0.0.0/0            0.0.0.0/0
```

删除已添加的iptables规则

将所有iptables以序号标记显示，执行：

```
iptables -L -n --line-numbers
```

比如要删除INPUT里序号为8的规则，执行：

```
iptables -D INPUT 8
```

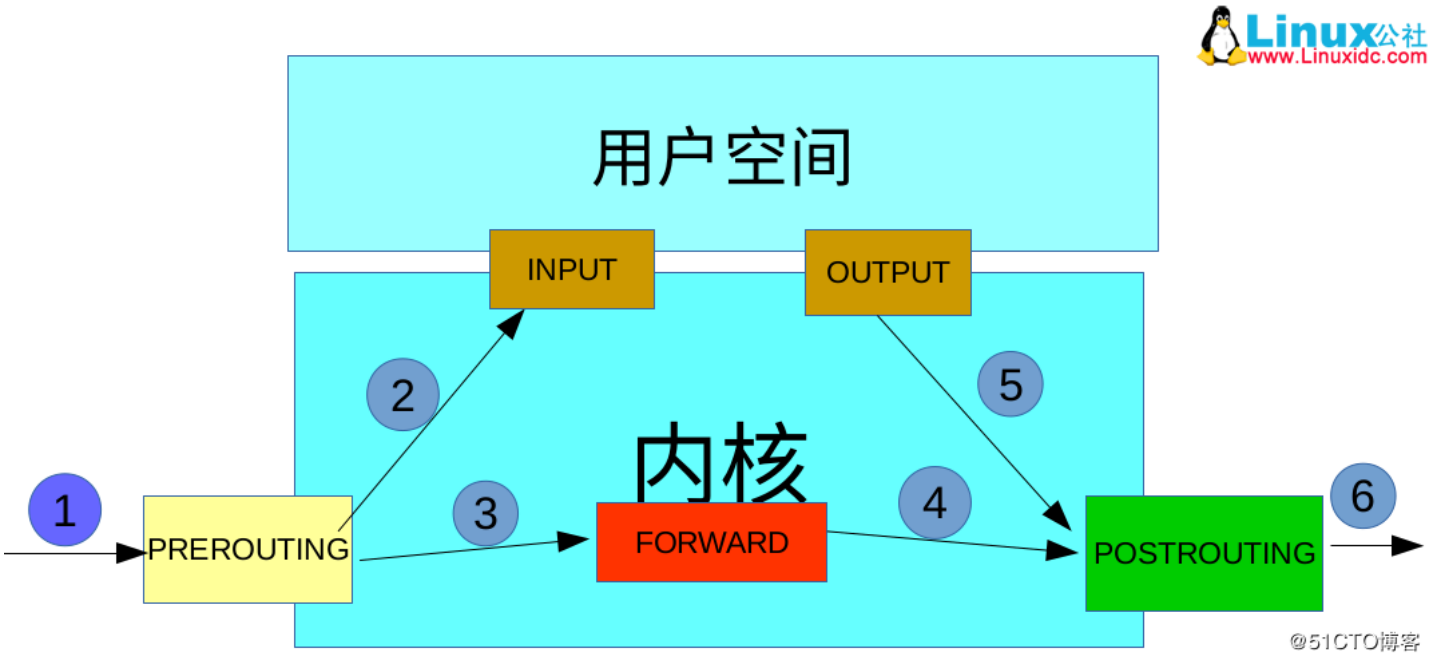
前提基础：
1、当主机收到一个数据包后，数据包先在内核空间中处理，若发现目的地址是自身，则传到用户空间中交给对应的应用程序处理，若发现目的不是自身，则进行转发。

2、iptables实现防火墙功能的原理是：在数据包经过内核的过程中有五处关键地方，分别是**PREROUTING、INPUT、OUTPUT、FORWARD、POSTROUT**子函数，iptables这款用户空间的软件可以在这5处地方写规则，对经过的数据包进行处理，规则一般的定义为“如果数据包头符合这样的条件，就这样处理数

3、iptables中定义有5条链，说白了就是上面说的5个钩子函数，因为每个钩子函数中可以定义多条规则，每当数据包到达一个钩子函数时，iptables就会从钩条规则开始检查，看该数据包是否满足规则所定义的条件。如果满足，系统就会根据该条规则所定义的方法处理该数据包；否则iptables将继续检查下一条规据包不符合钩子函数中任一条规则，iptables就会根据该函数预先定义的默认策略来处理数据包

4、iptables中定义有表，分别表示提供的功能，有filter表（实现包过滤）、nat表（实现网络地址转换）、mangle表（实现包修改）、raw表（实现数据跟踪一定的优先级：**raw-->mangle-->nat-->filter**

一条链上可定义不同功能的规则，检查数据包时将根据上面的优先级顺序检查



1、目的地址是本地，则发送到INPUT，让INPUT决定是否接收下来送到用户空间，流程为①--->②;

2、若满足PREROUTING的nat表上的转发规则，则发送给FORWARD，然后再经过POSTROUTING发送出去，流程为： ①--->③--->④--->⑥

主机发送数据包时，流程则是⑤--->⑥

iptables安装配置

linux一般默认都已经安装iptables，只需要开启服务即可

service iptables start //启动

service iptables restart //重启

service iptables stop //关闭

iptables规则书写：

基本语法：**iptables [-t 表] [操作命令] [链] [规则匹配器] [-j 目标动作]**

表	说明	支持的链

raw	一般是为了不再让iptables对数据包进行跟踪，提高性能	PREROUTING、OUTPUT
mangle	对数据包进行修改	五个链都可以
nat	进行地址转换	PREROUTING、OUTPUT、POSTROUTING
filter(默认)	对包进行过滤	INPUT、FORWARD、OUTPUT

常用操作命令	说明
-A	在指定链尾部添加规则
-D	删除匹配的规则
-R	替换匹配的规则
-I	在指定位置插入规则(例：iptables -I INPUT 1 --dport 80 -j ACCEPT（将规则插入到filter表INPUT链中的第一位上）
-L/S	列出指定链或所有链的规则
-F	删除指定链或所有链的规则
-N	创建用户自定义链[例：iptables -N allowed]
-X	删除指定的用户自定义链
-P	为指定链设置默认规则策略，对自定义链不起作用
-Z	将指定链或所有链的计数器清零
-E	更改自定义链的名称[例：iptables -E allowed disallowed]
-n	ip地址和端口号以数字方式显示[例：iptables -nL]

常用规则匹配器	说明
-p tcp/udp/icmp/all	匹配协议，all会匹配所有协议
-s addr[/mask]	匹配源地址
-d addr[/mask]	匹配目标地址
--sport port1[:port2]	匹配源端口(可指定连续的端口)
--dport port1[:port2]	匹配目的端口(可指定连续的端口)
-o interface	匹配出口网卡，只适用FORWARD、POSTROUTING、OUTPUT(例：iptables -A FORWARD -o eth0)
-i interface	匹配入口网卡，只使用PREROUTING、INPUT、FORWARD。
--icmp-type	匹配icmp类型（使用iptables -p icmp -h可查看可用的ICMP类型）
--tcp-flags mask comp	匹配TCP标记，mask表示检查范围，comp表示匹配mask中的哪些标记。（例：iptables -A FORWARD -p tcp --tcp-flags ALL SYN，ACK -j ACCEPT和ACK标记的数据包）

目标动作	说明
ACCEPT	允许数据包通过
DROP	丢弃数据包
REJECT	丢弃数据包，并且将拒绝信息发送给发送方
SNAT	源地址转换（在nat表上）例：iptables -t nat -A POSTROUTING -d 192.168.0.102 -j SNAT --to 192.168.0.1

DNAT	目标地址转换（在nat表上）例：iptables -t nat -A PREROUTING -d 202.202.202.2 -j DNAT --to-destination 192.168.0.102
REDIRECT	目标端口转换（在nat表上）例：iptables -t nat -D PREROUTING -p tcp --dport 8080 -i eth2.2 -j REDIRECT --to 80
MARK	将数据包打上标记;例：iptables -t mangle -A PREROUTING -s 192.168.1.3 -j MARK --set-mark 60

PS：
1、目标地址转换一般在PREROUTING链上操作
2、源地址转换一般在POSTROUTING链上操作

保存和恢复iptables规则

使用iptables-save可以保存到特定文件中

iptables-save >/etc/sysconfig/iptables_save

使用iptables-restore可以恢复规则

iptables-restore</etc/sysconfig/iptables_save

---

iptables的进阶使用
1、limit限制流量：
-m limit --limit 1000/s #设置最大平均匹配速率
-m limit --limit-burst 15 #设置一开始匹配的最大数据包数量
-m limit --limit 5/m --limit-burst 15 #表示一开始能匹配的数据包数量为15个，每匹配到一个，limit-burst的值减1,所以匹配到15个时，该值为0,以后每过12s，会加1,表示又能匹配1个数据包
例子：

iptables -A INPUT -i eth0 -m limit --limit 5/m --limit-burst 15 -j ACCEPT

iptables -A INPUT -i eth0 -j DROP

注意要点：

A、--limit-burst的值要比--limit的大

B、limit本身没有丢弃数据包的功能，因此，需要第二条规则一起才能实现限速的功能

2、time ： 在特定时间内匹配

-m time	**说明**
--monthdays day1[,day2]	在每个月的特定天匹配
--timestart hh:mm:ss	在每天的指定时间开始匹配
--timestop hh:mm:ss	在每天的指定时间停止匹配
--weekdays day1[,day2]	在每个星期的指定工作日匹配，值可以是1-7

例子：

iptables -A INPUT -i eth0 -m time --weekdays 1,2,3,4 -jACCEPT

iptables -A INPUT -i eth0 -j DROP

3、ttl：匹配符合规则的ttl值的数据包

参数	**说明**
--ttl -eq 100	匹配TTL值为100的数据包

--ttl -gt 100	匹配TTL值大于100的数据包
--ttl -lt 100	匹配TTL值小于100的数据包

例子：

iptables -A OUTPUT -m ttl --ttl-eq 100 -j ACCEPT

4、multiport：匹配离散的多个端口

参数	说明
--sports port1[,port2,port3]	匹配源端口
--dports port1[,port2,port3]	匹配目的端口
--ports port1[,port2,port3]	匹配源端口或目的端口

例子：

iptables -A INPUT -m multiport --sports 22，80，8080 -j DROP

5、state：匹配指定的状态数据包

参数	说明
--state value	value可以为NEW、RELATED（有关联的）、ESTABLISHED、INVALID（未知连接）

例子：

iptables -A INPUT -m state --state NEW，ESTABLISHED -j ACCEPT

6、mark：匹配带有指定mark值的数据包

参数	说明
--mark value	匹配mark标记为value的数据包

例子：

iptables -t mangle -A INPUT -m mark --mark 1 -j DROP

7、mac：匹配特定的mac地址

例子：

iptables -A FORWARD -m mac --mac-source 00:0C:24:FA:19:80 -j DROP

iptables详解 阅读数 708

看完下面这个iptables的讲解一下子豁然开朗，写的很详细一：前言防火墙，其实说白了讲，就是用于… 博文 来自： wdt3385的专栏

Linux服务器防火墙Iptables命令使用详解 阅读数 2667

iptables-AINPUT-s192.168.109.10-jDROP：拒绝192.168.109.10主机访问本服务器；注意：-A：添加… 博文 来自： han156的博客

iptables 详解 阅读数 8113

目录防火墙简介iptables与firewalldiptables基础3.1链的概念3.2表的概念3.3链与表的关系3.4数据通过的… 博文 来自： Choco Lee 的…

iptables基本原理和规则配置 阅读数 664

iptables原理图1.表的作用Mangle：打个标记，更改ttl值，更改查看tosNat：做DNAT、SNAT和端口映… 博文 来自： 鹏

iptables超全详解 阅读数 761

数据包先经过PREOUTING，由该链确定数据包的走向： 1、目的地址是本地，则发送到INPUT，让IN… 博文 来自： 三口酥屋

iptables命令详解--包括高级用法 阅读数 275

iptables配置文件直接改iptables配置就可以了：vim/etc/sysconfig/iptables。1、关闭所有的INPUTFOR… 博文 来自： sinat_2726162…

iptables从入门到应用 阅读数 95

iptables从入门到应用一、简介1.1、是什么？iptables是隔离主机以及网络的工具，通过自己设定的规… 博文 来自： weixin_33858…

Linux下iptables 禁止端口和开放端口 阅读数 16万+

iptables禁止端口和开放端口（转载）1、关闭所有的INPUTFORWARDOUTPUT只对某些端口开放。… 博文 来自： 海涛的博客

iptables 阅读数 97

iptables命令是Linux上常用的防火墙软件，是netfilter项目的一部分。可以直接配置，也可以通过许多前… 博文 来自： 破茧

iptables超全详解 - 三口酥屋 - CSDN博客

iptables详解 - u011029104的专栏 - CSDN博客

iptables基础 阅读数 666

原文：http://blog.coocla.org/207.htmliptables防火墙可以用于创建过滤(filter)与NAT规则。所有Linux发… 博文 来自： Tony的专栏

iptables详解 - 恋上蛋炒面的专栏 - CSDN博客

iptables详解(1):iptables概念 - firehive的博客 - CSDN博客

iptables简介 自定义链 阅读数 3540

iptables简介自定义链 博文 来自： lbyyy的专栏

wdt3385
1281篇文章
关注 排名:1000+

han156
39篇文章
关注 排名:千里之外

chocolee911
23篇文章
关注 排名:千里之外

迷茫十字路
190篇文章
关注 排名:千里之外

iptables详解 - Vincent's tech blog - CSDN博客

IPTABLES - Larry的博客 - CSDN博客

iptables 命令介绍 阅读数 46

原文链接iptables防火墙可以用于创建过滤(filter)与NAT规则。所有Linux发行版都能使用iptables，因此… 博文 来自： weixin_33964…

Linux防火墙iptables的启动与关闭 阅读数 2万+

CentOS7[root@localhost~]#cat/etc/redhat-releaseCentOSLinuxrelease7.2.1511(Core)1.关闭firewall[ro… 博文 来自： bitterliquor的专栏

Iptables详解+实例 - 全栈空间 - CSDN博客

iptables 深度详解 - weixin_38859100的博客 - CSDN博客

iptables命令介绍 阅读数 48

ptables防火墙可以用于创建过滤(filter)与NAT规则。所有Linux发行版都能使用iptables，因此理解如何… 博文 来自： weixin_34004…

【转载】Iptables详解 - 外星人(waixingrenabc) - CSDN博客

iptables及其过滤规则 阅读数 916

1.iptables是Linux内核的一个模块，用以管理对网络设备（网卡）的访问，如路由过滤、端口转发、NA… 博文 来自： 成长的足迹

linux系统中查看已设置iptables规则 阅读数 54

1、iptables-L查看filter表的iptables规则，包括所有的链。filter表包含INPUT、OUTPUT、FORWARD… 博文 来自： weixin_34357…

执行iptables -P INPUT DROP后无法联网 阅读数 3080

使用iptables-PINPUTDROP来全部关掉input链路后，随之产生了一个很严重的问题，那么服务器本身… 博文 来自： u012114090的…

iptables如何删除一条规则 阅读数 2万+

-- 查找所有规则iptables -L INPUT --line-numbers-- 删除一条规则iptables -D INPUT 11（注意，这个11… 博文 来自： 坚持初心,方得…

防火墙简介 阅读数 10

一：前言 防火墙，其实说白了讲，就是用于实现Linux下访问控制的功能的，它分为硬件的或者软件的… 博文 来自： weixin_34387…

iptables基础（一） 阅读数 23

iptables指令语法：iptables[-ttable]command[match][-jtarget/jump]-t参数用来指定规则表，内建的规则… 博文 来自： weixin_33946…

iptables详解（1）：iptables概念 阅读数 263

http://www.zsythink.net/archives/1199 博文 来自： firehive的博客

docker、firewalld和iptables之间的关系 阅读数 748

要注意docker命令中使用-p暴露端口时，实现需要依赖iptables。CentOS7默认使用的是firewalld,但是… 博文 来自： Larry的博客

iptables 使用详解 阅读数 3959

iptables规则功能filter表:filter主要和主机自身有关，主要负责防火墙功能过滤本机流入流出的数据包是… 博文 来自： chengxuyuany…

Iptables介绍和实用使用方法 阅读数 1334

一、简介1）---> IPTABLES 是与最新的 3.5 版本 Linux 内核集成的 IP 信息包过滤系统,在redha… 博文 来自： cbuy888的博客

Linux iptables 详解 阅读数 142

1、安全优化大并发的情况下，不能开iptables。我们使用硬件防火墙，当然硬件防火墙也有一定的吞吐… 博文 来自： pang_2899的…

iptables防火墙规则的添加、删除、修改、保存 阅读数 4564

原文链接：http://www.splaybow.com/post/iptables-rule-add-delete-modify-save.html一、查看规则集ipt… 博文 来自： raquelle的记忆…

关于iptables添加规则不生效的问题 阅读数 2万+

1.我们要增加的规则是：-AINPUT-ptcp-mstate--stateNEW-mtcp--dport82-jACCEPT即开放82的tcp端口… 博文 来自： Lyndon的专栏

iptables服务 阅读数 1151

1.启用iptables[root@client~]#systemctlstopfirewalld.service[root@client~]#systemctldisablefirewalld.se... 博文 来自： lin_made的博客

分享靠写代码赚钱的一些门路 阅读数 2万+

作者mezod，译者josephchang10如今，通过自己的代码去赚钱变得越来越简单，不过对很多人来说依… 博文 来自： Python之禅的…

中国物联网激荡20年 阅读数 9903

故事还要从24年前那个夏天说起。**1**1995年的夏天，美国西海岸有一个中年人出版了一本叫《未来… 博文 来自： 边缘计算社区

前端开发必备网站推荐 阅读数 6488

本人是一个纯正的小白，在学习的过程中搜集了一些关于前端开发的网站，希望对大家能够有所帮助！… 博文 来自： 小白

【转载】Iptables详解 阅读数 329

Iptabels是与Linux内核集成的包过滤防火墙系统，几乎所有的linux发行版本都会包含Iptables的功能。… 博文 来自： 外星人（waixi…

iptable命令参数详解 阅读数 421

###还不够详细，后期补充###开放某端口：iptables-IINPUT-ptcp--dport9000-jACCEPT关闭某端口:ipt… 博文 来自： God丶Davide…

iptables 执行清除命令 iptables -F 要非常小心的 . 阅读数 178

用/sbin/iptables-F要小心，搞不好，你就马上同服务器断开连接了以下是来自http://wiki.ubuntu.org.cn/I… 博文 来自： weixin_34138…

写个最简单的植物大战僵尸修改器吧！c和python 阅读数 3715

效果图：C实现：#include<windows.h>#include<stdio.h>voidmain(){ //获取游戏窗口句柄 HW… 博文 来自： 吾无法无天的…

Google离开我们快十年了 阅读数 2万+

2010年1月13日，Google离开中国。掐指算来，Google已经离开我们快十年了。2010年是个特殊的年… 博文 来自： 阿朱=行业趋势…

docker学习笔记 阅读数 2267

docker学习笔记 常用的镜像: docker pull anibali/pytorch:cuda-10.0 Docker是什么？ Docker是一个虚拟… 博文

学会了这些技术，你离BAT大厂不远了 阅读数 2万+

每一个程序员都有一个梦想，梦想着能够进入阿里、腾讯、字节跳动、百度等一线互联网公司，由于身… 博文

程序员实用工具网站 阅读数 11万+

目录 1、搜索引擎 2、PPT 3、图片操作 4、文件共享 5、应届生招聘 6、程序员面试题库 7、办公、开… 博文

2019年9月中国编程语言排行榜 阅读数 7712

2019年9月2日，我统计了某招聘网站，获得有效程序员招聘数据9万条。针对招聘信息，提取编程语言… 博文

shell-【技术干货】工作中编写shell脚本实践 阅读数 1万+

在公司项目的开发过程中，需要编写shell脚本去处理一个业务，在编写过程中发现自身对shell脚本的知… 博文

挑战10个最难的Java面试题（附答案）【上】 阅读数 2万+

这是收集的10个最棘手的Java面试问题列表。这些问题主要来自 Java 核心部分 ,不涉及 Java EE 相关… 博文

我花了一夜用数据结构给女朋友写个H5走迷宫游戏 阅读数 6万+

起因 又到深夜了，我按照以往在csdn和公众号写着数据结构！这占用了我大量的时间！我的超越妹妹… 博文

别再翻了，面试二叉树看这 11 个就够了~ 阅读数 3万+

写在前边 数据结构与算法： 不知道你有没有这种困惑，虽然刷了很多算法题，当我去面试的时候，面… 博文

GitHub开源的10个超棒后台管理面板 阅读数 2万+

目录 1、AdminLTE 2、vue-Element-Admin 3、tabler 4、Gentelella 5、ng2-admin 6、ant-design-pro … 博文

100 个网络基础知识普及，看完成半个网络高手 阅读数 7万+

欢迎添加华为云小助手微信（微信号：HWCloud002或HWCloud003），验证通过后，输入关键字“加… 博文

对计算机专业来说学历真的重要吗? 阅读数 2万+

我本科学校是渣渣二本，研究生学校是985，现在毕业五年，校招笔试、面试，社招面试参加了两年了… 博文

C语言实现推箱子游戏 阅读数 4万+

很早就想过做点小游戏了，但是一直没有机会动手。今天闲来无事，动起手来。过程还是蛮顺利的，代… 博文

面试官：兄弟，说说基本类型和包装类型的区别吧 阅读数 2万+

Java 的每个基本类型都对应了一个包装类型，比如说 int 的包装类型为 Integer，double 的包装类型为 … 博文

一些实用的GitHub项目 阅读数 2万+

最近整理了一些在GitHub上比较热门的开源项目关于GitHub，快速了解请戳这里其中涵盖了：学习教… 博文

新手程序员成长之路的五本必读书籍（附资源下载） 阅读数 2万+

全文共3351字，预计学习时长7分钟图片来自Pixabay，IvanPais书籍可以清晰而有条理地陈诉观点，纸… 博文

30秒内便能学会的30个超实用Python代码片段 阅读数 2万+

许多人在数据科学、机器学习、web开发、脚本编写和自动化等领域中都会使用Python，它是一种十分… 博文

python入门的120个基础练习 阅读数 1万+

python入门的120个基础练习 解决问题的道路上， " 方法 " 和 " 坚持 " 缺一不可。 ----------… 博文

JAVA-快速了解线程池的基本原理 阅读数 3179

前言 说起线程池大家肯定不会陌生，在面试中属于必问的问题之一，特别是对于高并发有较高要求的… 博文

失败程序员的十年总结 阅读数 4535

十年到底有多长？当我回顾过去的十年，发现好短，可以讲的事情没有几件，而且都是坏事；当我畅想… 博文

Python搭建代理IP池（一）- 获取 IP 阅读数 2654

使用爬虫时，大部分网站都有一定的反爬措施，有些网站会限制每个 IP 的访问速度或访问次数，超出… 博文

可视化越做越丑？这五个高级图表效果能瞬间抬升你的逼格 阅读数 5096

今天我们来说一说数据可视化，想必很多人在入门数据分析之后，就会经常进行可视化的工作，所谓一… 博文

感觉自己不会的东西太多了，不知道如何下手? 阅读数 7616

GitHub 8.8k Star 的Java工程师成神之路 ，不来了解一下吗? GitHub 8.8k Star 的Java工程师成神之路 … 博文

别死写代码了，方法比结果更重要 阅读数 1751

点击上方“程序猿技术大咖”，选择“关注公众号”，一起共进步！如果每个程序开发人员都只是周而复始… 博文

为什么程序员在学习编程的时候什么都记不住? 阅读数 5186

在程序员的职业生涯中，记住所有你接触过的代码是一件不可能的事情！那么我们该如何解决这一问题… 博文

成长的第一步是走出舒适区 阅读数 6118

阅读本文大概需要 2.8 分钟。在温室里呆习惯了，就很难去适应室外环境，在一个圈子呆久了，就会把… 博文

记录一次九月份腾讯 Android 面试笔试总结（面试题详细答案解析） 阅读数 4991

今天把之前九月份腾讯面试笔试题目整理出来给大家分享分享，还附上了我自己的一些答案解析，给大… 博文

一道90%都会做错的指针题 阅读数 2270

今天，在我们的一个小群里，一个同学发了一道题目给我看，这道题目应该是C语言面试的一股清流了… 博文

牛逼，送大家一个网络共享的必备梯子，你懂得 阅读数 2049

【公众号回复 “1024”，免费领取程序员赚钱实操经验】今天给大家推荐的这个开源项目，是来自于读者… 博文

扛住阿里双十一高并发流量，Sentinel是怎么做到的? 阅读数 5395

Sentinel 承接了阿里巴巴近 10 年的双十一大促流量的核心场景本文介绍阿里开源限流熔断方案 Sentin… 博文

500行代码，教你用python写个微信飞机大战 阅读数 1万+

这几天在重温微信小游戏的飞机大战，玩着玩着就在思考人生了，这飞机大战怎么就可以做的那么好，… 博文

唐僧团队要裁员，你会裁谁? 阅读数 9289

提问： 西游记取经团为了节约成本，唐太宗需要在这个团队里裁掉一名队员，该裁掉哪一位呢，为什… 博文

大数据学习之Linux基础 阅读数 2971

大数据学习之Linux基础 自定义Linux虚拟机安装网络配置1.node1网络配置2.通过快照克隆虚拟机3.配… 博文

5大优秀黑客必逛技术网站 阅读数 3395

5大优秀黑客必逛技术网站 Hack Forums 最理想的黑客技术学习技术根据地，也适用于开发人员游戏开… 博文

python 实现十大排序算法 阅读数 2466

冒泡排序 这个算法的名字由来是因为越小的元素会经由交换慢慢“浮”到数列的顶端。 算法过程： 进行… 博文

红黑树详细分析 阅读数 3142

文章目录红黑树简介红黑树的性质红黑树操作旋转操作插入情况一情况二情况三情况四情况五插入总结… 博文

史上最全的中高级JAVA工程师-面试题汇总 阅读数 1万+

史上最全的java工程师面试题汇总，纯个人总结，精准无误。适合中高级JAVA工程师。... 博文

金九银十收获阿里腾讯实习offer，学习、面试经验分享 阅读数 1937

今天分享一位大学生实习的面经，再结合我自己的经验总结一些看法和学习方法，希望能对大家有帮助… 博文

为啥程序员下班后只关显示器从不关电脑? 阅读数 2073

点击上方“程序猿技术大咖”，选择“关注公众号”，一起共进步！首百问答的答案：jingmentudou因为你… 博文

前端开发大师修炼指南 阅读数 2720

如果你想成为一名专业的JavaScript开发人员，那么除了掌握JavaScript之外，至少还应该具备一些其… 博文

为什么这么多人说 IDEA 比 Eclipse 更好? 阅读数 1360

点击上方“黄小斜”，选择“置顶或者星标”一起成为更好的自己！作者：彭博来源：http://1t.click/asZu# … 博文

c# 去除空格 c#读取tiff未bmp c# 识别回车 c#生成条形码ean13 c#子控制器调用父控制器 c# 写大文件 c# 浏览pdf c#获取桌面图标的句柄 c# list反射 c# 句柄 进程