

转

iptables基础知识详解

2016年02月19日 14:42:31

阅读数：10496

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。如果你是第一次接触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。

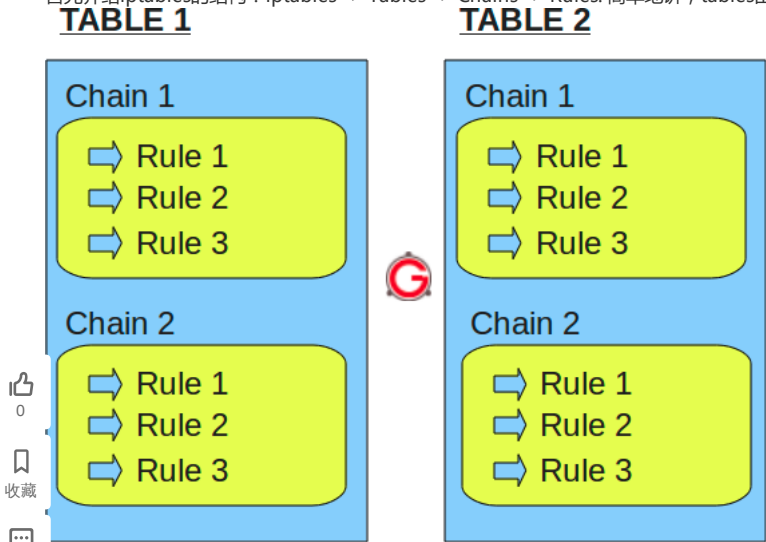


图: IPTables Table, Chain, and Rule Structure

#### 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 NAT)。
- **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

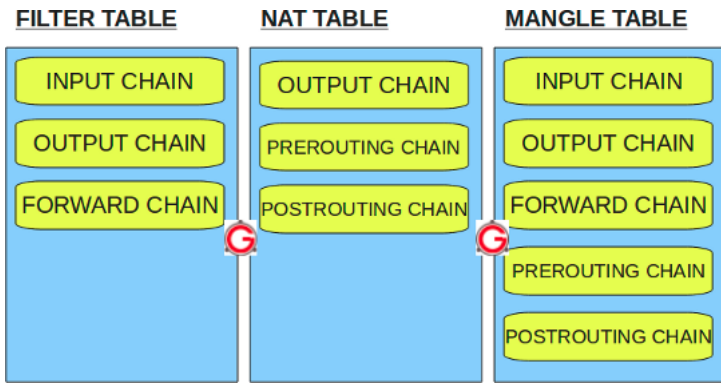


图: IPTables 内建表

## 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, forward链, 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
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
3	ACCEPT	esp	—	0.0.0.0/0	0.0.0.0/0

```
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
3	ACCEPT	esp	—	0.0.0.0/0	0.0.0.0/0

```

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，此时只能手动清除：

```
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。下面进行简单介绍：

#### 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**

- 参数和-s相同
- 还可以使用--dst或者--destination

#### -j 执行目标 ( jump to target )

- -j代表“ jump to target”
- -j指定了当与规则(Rule)匹配时如何处理数据包
- 可能的值是ACCEPT, DROP, QUEUE, RETURN , **MASQUERADE**
- 还可以指定其他链 ( Chain ) 作为目标
- 注：**MASQUERADE**，地址伪装，算是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 输入接口 ( input interface )

- -i代表输入接口(input interface)
- -i指定了要处理来自哪个接口的数据包
- 这些数据包即将进入INPUT, FORWARD, PREROUTE链
- 例如：**-i eth0**指定了要处理经由eth0进入的数据包
- 如果不指定-i参数，那么将处理进入所有接口的数据包
- 如果出现! -i eth0，那么将处理所有经由**eth0以外的接口**进入的数据包
- 如果出现-i eth+，那么将处理所有经由**eth开头的接口**进入的数据包
- 还可以使用--in-interface参数

#### -o 输出 ( out interface )

- -o代表“ output interface”
- -o指定了数据包由哪个接口输出
- 这些数据包即将进入FORWARD, OUTPUT, POSTROUTING链
- 如果不指定-o选项，那么系统上的所有接口都可以作为输出接口
- 如果出现! -o eth0，那么将从**eth0以外的接口**输出
- 如果出现-i eth+，那么将仅从**eth开头的接口**输出
- 还可以使用--out-interface参数

### 3.描述规则的扩展参数

对规则有了一个基本描述之后，有时候我们还希望指定端口、TCP标志、ICMP类型等内容。

#### --sport 源端口 ( source port ) 针对 -p tcp 或者 -p udp

- 缺省情况下，将匹配所有端口
- 可以指定端口号或者端口名称，例如“ --sport 22”与“ --sport ssh”。
- /etc/services文件描述了上述映射关系。
- 从性能上讲，使用端口号更好
- 使用冒号可以匹配端口范围，如“ --sport 22:100”
- 还可以使用“ --source-port”

#### --dport 目的端口 ( destination port ) 针对-p tcp 或者 -p udp

- 参数和--sport类似
- 还可以使用“ --destination-port”

#### --tcp-flags TCP标志 针对-p tcp

- 可以指定由逗号分隔的多个参数
- 有效值可以是：SYN, ACK, FIN, RST, URG, PSH
- 可以使用**ALL**或者**NONE**

#### --icmp-type ICMP类型 针对-p icmp

- --icmp-type 0 表示Echo Reply
- --icmp-type 8 表示Echo

### 4.追加规则的完整实例：仅允许SSH服务

本例实现的规则将仅允许SSH数据包通过本地计算机，其他一切连接（包括ping）都将被拒绝。

# 1.清空所有iptables规则

```
iptables -F
```

# 2.接收目标端口为22的数据包

```
iptables -A INPUT -i eth0 -p tcp --dport 22 -j ACCEPT
```

# 3.拒绝所有其他数据包

```
iptables -A INPUT -j DROP
```

### 六、更改默认策略

上例的例子仅对接收的数据包过滤，而对于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. 默认链策略

/!\警告：请勿在远程连接的服务器、虚拟机上测试！

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：

```
# iptables -L
```

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

```
ACCEPT  tcp -- anywhere      anywhere      tcp dpt:ssh
DROP    all  -- anywhere      anywhere
```

Chain FORWARD (policy ACCEPT)

```
target  prot opt source      destination
```

Chain OUTPUT (policy ACCEPT)

```
target  prot opt source      destination
```

这种情况下，如果没有明确添加DROP规则，那么默认情况下将采用ACCEPT策略进行过滤。除非：

**a)为以上三个链单独添加DROP规则：**

```
iptables -A INPUT -j DROP
iptables -A OUTPUT -j DROP
iptables -A FORWARD -j DROP
```

**b)更改默认策略：**

```
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
```

糟糕！！如果你严格按照上一节的例子配置了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。本节在上一节基础上，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，并检查数据包的状态字段。

### 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
```

```
# 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
```

个人分类：Linux

查看更多>>

想对作者说点什么？ 我来说两句

 zhushuangyin 2017-03-30 10:12:59 #1楼  
我尽量以通俗易懂的方式总结了iptables的概念，欢迎交流 <http://www.zsythink.net/archives/1199>

上一页 1 下一页

iptables详解

Netfilter包含有三种表，三种表下共包含有五种链，链下面包含各种规则。即表包含若干链，链包含若干规则。（一）三种表为：filter nat mangle 1、filter: 处理...

 Primeprime 2016-09-04 20:29:15 阅读数：2174

Iptables详解

Iptables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。如果 Linux 系统连接到因特网或 LAN、服务器或连接 LAN 和因特网的代理...

 reyleon 2013-10-23 18:54:38 阅读数：42682

iptables详解 - CSDN博客

iptables简介 netfilter/iptables(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...  
2018-5-19

超级详细的iptables介绍 - CSDN博客

Iptables 指南 1.1.19Oskar Andreasson oan@frozentux.netCopyright © 2001-2003 by ...  
2018-5-3

民间办法让你延长30分钟，当心对象受不了

安邦车·顶新

关于IPTABLES 各种MARK 功能的用法

1、 iptalbes 的有多个MARK 模块..用法各不相同..一直没有完全明白..希望高手解释一下各功能的使用及区别.... -m mark -m connmark -j MARK -j CONN...

## iptables命令框架结构图

iptables命令框架结构图 iptables命令框架结构图 iptables命令框架结构图 综合评分:0 收藏评论举报 所需: 3积分/C币 下载个数: 14 开通VIP 立即下载 ...

2018-5-8

## iptables基本原理 - CSDN博客

iptables实现防火墙功能的原理是:在数据包经过内核的过程...数据结构 1篇 IPsec 2篇 PPPoE 1篇 PPTP 3篇 React 8篇 HTML 2篇...

2018-6-6

## Linux中iptables设置详细

无论如何，iptables是一个需要特别谨慎设置的东西，万一服务器不在你身边，而你贸然设置导致无法SSH，那就等着被老板骂吧，呵呵。。。一下内容是为了防止这种情况发生而写的，当然很初级，不过一般服务...

 guochunyang 2015-11-16 14:23:53 阅读数：55720

## iptables 使用详解

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默认使用的表; input :负责过滤所有目标地址是...

 chengxuyuanonghu 2016-07-13 16:11:13 阅读数：1542

## iptables详解 - CSDN博客

source: <http://www.cnblogs.com/metoy/p/4320813.html> iptables简介 netfilter/iptables(简称为iptables)组成Linux平台下的包过滤防火墙,...

2018-5-29

## iptables防火墙原理详解 - CSDN博客

原文地址:<http://seanlook.com/2014/02/26/iptables-example/> 1. netfilter与iptables Netfilter是由Rusty Russell提出的Linux 2.4内核防火墙框架,该框架既简洁又灵活...

2018-6-6

## Linux防火墙iptables详解(三)--iptables命令详解和举例

Linux防火墙iptables详解

 makyen 2016-06-27 17:13:54 阅读数：253

## 如何满足女人30分钟？男人们都应该看！

苏装 · 顶新

## iptables详解 - CSDN博客

文章转载:<http://www.cnblogs.com/metoy/p/4320813.html> 点击打开链接 iptables详解 iptables简介 netfilter/iptables(简称为iptables)组成Linux平台下的包过滤防火墙,...

2018-5-27

## iptables详解 - CSDN博客

转自<http://www.cnblogs.com/metoy/p/4320813.html> iptables简介 netfilter/iptables(简称为iptables)组成Linux平台下的包过滤防火墙,与大...

2017-12-6

## iptables防火墙原理详解

原文地址:<http://seanlook.com/2014/02/26/iptables-example/> 1. netfilter与iptables Netfilter是由Rusty Russell...

 silent123go 2016-09-19 19:20:58 阅读数：2432

## linux网络防火墙-iptables配置详解

如果你的IPTABLES基础知识还不了解,建议先去IPTABLES基础. 开始配置 我们来配置一个filter表的防火墙. (1)查看本机关于IPTABLES的设置情况 [root@tp ~]# i...



iptables详解 - CSDN博客

iptables简介 netfilter/iptables(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...  
2017-11-26

undefined

Linux iptables详解

内容简介 防火墙的概述 iptables简介 iptables基础 iptables语法 iptables实例 案例详解 防火墙的简介 防火墙是指设置在不同网络或网络安...  
kklvsports 2014-04-01 19:46:10 阅读数：4091

Iptables 详解

1：iptables - Layer7 iptables默认是OSI三层和四层以及二层源MAC地址过滤 针对于某一个应用：xunlei，kugou，qq，msn，flv，p2p，http...  
wh211212 2016-11-29 10:13:27 阅读数：950

calico iptables详解

报文处理过程 报文处理过程中使用的标记位： 一共使用了3个标记位，0x7000000对应的标记位 0x1000000: 报文的处理动作，置1表示放行，默认0表示拒绝。 0x2000000: 是...  
ptmozhu 2017-06-15 19:45:06 阅读数：1958

Linux防火墙iptables详解(二)--参数指令

Linux防火墙iptables详解  
makyan 2016-06-27 16:49:03 阅读数：1016

linux 中防火墙配置 iptables 命令参数的含义介绍

点我进入原文 iptables 命令介绍 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ipt...  
zhyh1435589631 2016-04-01 14:09:18 阅读数：3593

花1元学新技能！抢课原价99，限时福利>

学费1元！多语种课程点击抢购>>仅限今天



iptables基础知识

iptables由3个表filter，nat，mangle组成，主要实验了filter表，这个表是用来过滤数据包的，有三个链INPUT,OUTPUT,FORWARD。配置防火墙策略有固...  
chengxuyuanonghu 2016-07-13 12:06:25 阅读数：842

iptables基本原理

前提基础： 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，则会将包丢弃或进行转发。 ...  
naipeng 2017-05-04 10:04:06 阅读数：529

linux网络防火墙-iptables基础详解

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防火墙两种。无论是在哪个网络中，防火墙工作的地方一定是在网络的边缘。而我们的任务就是需要去定义到...  
wlzx120 2016-08-24 15:22:43 阅读数：7092

iptables中的return

1. 从一个CHAIN里可以jump到另一个CHAIN，jump到的那个CHAIN是子CHAIN. 2. 从子CHAIN return后，回到触发jump的那条规则，从那条规则的下一条继续匹配. ...  
wsclinux 2016-11-21 09:55:31 阅读数：2830

iptables



 tanzhe7

2014-11-08 18:50:48

阅读数：640

## 便宜云虚拟主机

云虚拟主机价格表

百度广告



## iptables 从链、表开始理解

转自：<https://my.oschina.net/HankCN/blog/117796> Filter表：过滤数据包，默认表。（1）INPUT...

 wsclinux

2016-11-14 19:49:23

阅读数：736

## Iptables

一 iptables规则原理和组成 1.iptables:将规则组成一个列表，实现绝对详细的访问控制功能。其实就是一个定义规则的工具，让在内核空间当中的netfilter（网络过滤器）...

 HzSunshine

2017-01-31 21:14:01

阅读数：807

## IPTABLES入门

声明：由于查看网上资料发现无法满足我的理解能力（理解能力太差），总结的不系统（不满足我要的要求），所以将iptables总结与此，转载可以不留名，但是我相信有JJ的都会留名。纯粹菜鸟级别，大神请绕道。...

 u013660039

2014-02-19 16:23:41

阅读数：642

## iptables基础知识.详解

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。如果你是第一次...

 night\_elf\_1020

2014-05-16 10:56:54

阅读数：1292

## linux下IPTABLES配置详解

-A RH-Firewall-1-INPUT -p tcp -m state --state NEW -m tcp --dport 24000 -j ACCEPT -A RH-Firewall-1-I...

 dreamboyxcx

2017-12-04 10:25:48

阅读数：155

## 【1元报班】学小语种课程！仅限今天！

多语种课程1元就上课!学小语种！变更优秀



## 超级详细的iptables介绍

Iptables 指南 1.1.19Oskar Andreasson oan@frozentux.netCopyright © 2001-2003 by Oskar Andreasson 本文...

 sdytlm

2011-06-14 22:37:00

阅读数：27604

## iptables简介文档

2017年08月20日

144KB

下载



## iptables常用命令及应用

一、命令格式 iptables [-t TABLE] COMMAND CHAIN [criteria] -j(jump) ACTION{ACCEPT,DROP,REJECT,SNAT,DNAT}...

 gzhouc

2016-07-22 17:48:08

阅读数：759

## iptables之FORWARD转发链

注意：本机路由转发的时候，才配置FORWARD转发链！#iptables -A FORWARD -s 192.168.0.0/24 -j ACCEPT #iptables...

 foreverfriends

2017-04-18 14:11:58

阅读数：3991

## Iptables之FORWARD转发链

图有借鉴意义 本机路由转发的时候，才配置FORWARD转发链~！# iptables -A FORWARD -s 192.168.0.0/24 -j ACCEPT # iptab...

运维管理系统

智能运维管理系统设计方案

百度广告



iptables命令详解和举例

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防火墙两种。无论是在哪个网络中，防火墙工作的地方一定是在网络的边缘。而我们的任务就是需要去定义到底防火墙如...

qq\_38892883 2018-03-27 10:25:47 阅读数：20

Linux防火墙iptables学习笔记（三）iptables命令详解和举例

网上看到这个配置讲解得还比较易懂，就转过来了，大家一起看下，希望对您工作能有所帮助。网管员的安全意识要比空喊Linux安全重要得多。iptables -F ip tables -X ip...

liujianminghero 2015-12-06 21:13:39 阅读数：2492

Linux防火墙iptables学习笔记（一）入门要领

要在网上传输的数据会被分成许多小的数据包，我们一旦接通了网络，会有很多数据包进入，离开，或者经过我们的计算机。首先我们要弄明白，防火墙将怎么对待这些数据包。这些数据包会经过一些相应...

wailaizhu 2016-12-08 18:06:08 阅读数：1598

iptables的使用方法（带常用实例）

1、iptables 的基本用法说明 保存.写入到/etc/sysconfig/iptables文件里 iptables-save >/etc/sysconfig/iptables /etc...

u013485792 2016-08-23 15:10:48 阅读数：639

Iptables服务全攻略之实战

Iptables原理 现在防火墙主要分以下三种类型：包过滤、应用代理、状态检测 包过滤防火墙：现在静态包过滤防火墙市面上已经看不到了，取而代之的是动态包过滤技术的防火墙哈~ 代理防火墙：因一些特...

Al\_xin 2014-09-15 23:03:42 阅读数：1252

1元学外语！点击抢课>7天说流利小语种！

这些课真的只要1元！12国外语随时学！



CentOS防火墙iptables的配置方法详解

iptables是与Linux内核集成的IP信息包过滤系统，其自带防火墙功能，我们在配置完服务器的角色功能后，需要修改iptables的配置。配置CentOS和Ubuntu等Linux服务器时需要...

wailaizhu 2016-12-06 16:43:07 阅读数：31459

Iptables工具的使用

Iptables工具的使用...

junjieguo 2012-04-10 21:13:39 阅读数：3628

iptables的interface更新

经常设置iptables规则的人都知道，设置接口的时候。比如：iptables -i eth0.1 -s 192.168.8.99 -j DROP 有的时候是pppoe拨号，会规则会变成这样i...

zbffff 2015-10-08 17:15:07 阅读数：641

iptables详解

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防火墙两种。无论是在哪个网络中，防火墙工作的地方一定是在网络的边缘。而我们的任务就是需要去定义到底防火墙如...

qq\_21816375 2017-10-12 09:40:15 阅读数：109

 chen\_jianjian

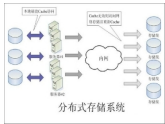
2015-09-11 16:01:38

阅读数：3029

## 分布式设计与开发

分布式

百度广告



## iptables--命令行解析

一、iptables命令行初探：在linux下执行iptables --help iptables --help iptables v1.4.21 Usage: ip...

 xiakewudi

2017-09-01 11:36:30

阅读数：408

## iptables 指令详解

iptables 指令 语法：iptables [-t table] command [match] [-j target/jump] -t 参数用来指定规则表，内建的规则表有三个，分别是：nat、...

 qinglinsan

2016-05-15 22:11:53

阅读数：641

## Iptables的规则语法

(一) 基本语法 iptables-t filter -A INPUT -p icmp -j DROP 高级语法 iptables-t filter -A INPUT -m mac --mac-...

 junjieguo

2012-04-19 17:09:26

阅读数：6671

## iptables语法总结

iptables SyntaxAs presented earlier, iptables uses the concept of separate rule tables for different...

 zzulp

2010-05-22 23:49:00

阅读数：3015

## 2\_小时玩转 iptables\_企业版\_v1.6.0 (重点：iptables语法概述)

2016年05月02日

1.36MB

下载



## 50万码农评论：英语对于程序员有多重要？

不背单词和语法，一个公式学好英语



## 如何用iptables开放一段端口

你要是想开放一段，比如6000~6500，那就用冒号连接 iptables -A INPUT -p tcp -dport 6000:6500 -j ACCEPT...

 kepa520

2015-11-11 16:31:17

阅读数：818

没有更多推荐了，[返回首页](#)

### 个人资料



splenday1989

关注

原创	粉丝	喜欢	评论
11	12	0	2

等级：	博客 4	访问：	9万+
积分：	1102	排名：	4万+



免费云主机试用一年



最新文章

- Firewall简介
- Centos7-firewall ( 初学转发及访问控制 )
- yum 查找需要想要安装的软件
- 设置Centos7的主机名称
- linux命令 ( 文件切割 )

个人分类

loadRunner	9篇
MongoDb	5篇
Linux	77篇
Python	3篇
Docker	1篇

展开

归档

2017年9月	4篇
2016年4月	1篇
2016年3月	4篇
2016年2月	3篇
2016年1月	2篇

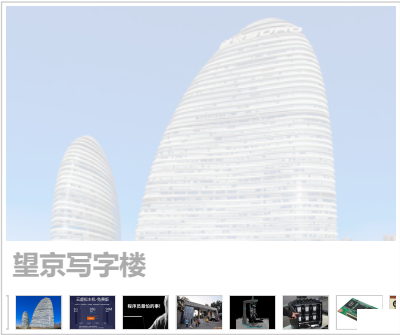
展开

热门文章

- Shell脚本中参数传递方法常用有8种  
阅读量：17257
- Samba配置详解  
阅读量：15798
- iptables基础知识详解  
阅读量：10459
- linux \$@和\$\*区别  
阅读量：3787
- LoadRunner11+Win7+IE8(64位)录制时没有弹出IE  
阅读量：3106

最新评论

- Centos7-firewall ( ...  
splenday：有大神知道怎么用Firewall代理上网的吗？
- iptables基础知识详解  
zz6547：我尽量以通俗易懂的方式总结了iptables



联系我们



请扫描二维码联系客服  
✉ webmaster@csdn.net  
☎ 400-660-0108  
👤 QQ客服 🗨 客服论坛

关于 招聘 广告服务 网站地图  
©2018 CSDN版权所有 京ICP证09002463号  
🔍 百度提供支持

经营性网站备案信息  
网络110报警服务  
中国互联网举报中心  
北京互联网违法和不良信息举报中心