A+

iptables详解（12）：iptables动作总结之一

在本博客中，从理论到实践，系统的介绍了iptables，如果你想要从头开始了解iptables，可以查看iptables文章列表，直达链接如下
iptables零基础快速入门系列

前文一直在介绍iptables的匹配条件，并没有对动作进行过总结，那么此处，我们就来总结一下iptables中的动作。
之前的举例中已经用到了一些常用动作，比如ACCEPT、DROP、REJECT等。
其实，"动作"与"匹配条件"一样，也有"基础"与"扩展"之分。
同样，使用扩展动作也需要借助扩展模块，但是，扩展动作可以**直接使用**，不用像使用"扩展匹配条件"那样指定特定的模块。

之前用到的ACCEPT与DROP都属于基础动作。
而REJECT则属于扩展动作。

之前举过很多例子，我们知道，使用-j可以指定动作，比如
-j ACCEPT
-j DROP
-j REJECT

其实，"动作"也有自己的选项，我们可以在使用动作时，设置对应的选项，此处以REJECT为例，展开与"动作"有关的话题。

动作REJECT

REJECT动作的常用选项为--reject-with
使用--reject-with选项，可以设置提示信息，当对方被拒绝时，会提示对方为什么被拒绝。
可用值如下
icmp-net-unreachable
icmp-host-unreachable
icmp-port-unreachable,
icmp-proto-unreachable
icmp-net-prohibited
icmp-host-pro-hibited
icmp-admin-prohibited
当不设置任何值时，默认值为icmp-port-unreachable。

我们来动手实践一下，在主机139上设置如下规则，如下图所示，当没有明确设置--reject-with的值时，默认提示信息为icmp-port-unreachable，即端口不可达之

```
[www.zsythink.net]#iptables -F
[www.zsythink.net]#iptables -t filter -I INPUT -p tcp --dport 22 -j ACCEPT
[www.zsythink.net]#iptables -A INPUT -j REJECT
[www.zsythink.net]#
[www.zsythink.net]#iptables -nvL INPUT
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
   21  1608 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22
   13  2936 REJECT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           reject-with icmp-port-unreac
[www.zsythink.net]#
```


此时在另一台主机上向主机139发起ping请求，如下图所示，提示目标端口不可达。

```
192.168.1.146:22
[www.zsythink.net]# ping 192.168.1.139
PING 192.168.1.139 (192.168.1.139) 56(84) bytes of data.
From 192.168.1.139 icmp_seq=1 Destination Port Unreachable
From 192.168.1.139 icmp_seq=2 Destination Port Unreachable
From 192.168.1.139 icmp_seq=3 Destination Port Unreachable
From 192.168.1.139 icmp_seq=4 Destinat
```


那么我们将拒绝报文的提示设置为"主机不可达"，示例如下

```
[www.zsythink.net]#iptables -nvL INPUT
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
  305 26568 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22
 6850  895K REJECT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           reject-with icmp-port-unreachab
[www.zsythink.net]#iptables -I INPUT 2 -j REJECT --reject-with icmp-host-unreachable
[www.zsythink.net]#iptables -nvL INPUT
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
  433 36712 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22
    6   468 REJECT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           reject-with icmp-host-unreachab
 7041  915K REJECT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           reject-with icmp-port-unreachab
[www.zsythink.net]#
```


如上图所示，我们在设置拒绝的动作时，使用了--reject-with选项，将提示信息设置为icmp-host-unreachable，完成上述操作后，我们再次在在另一台主机上向主ng请求。

如下图所示。

```
[www.zsythink.net]# ping 192.168.1.139
PING 192.168.1.139 (192.168.1.139) 56(84) bytes of data.
From 192.168.1.139 icmp_seq=1 Destination Host Unreachable
From 192.168.1.139 icmp_seq=2 Destination Host Unreachable
From 192.168.1.139 icmp_seq=3 Destination Host Unreachable
From 192.168.1.139 icmp_seq=4 Destinat
```


可以看到，ping请求被拒绝时，提示信息已经从"目标端口不可达"变成了"目标主机不可达"。

动作LOG

在本博客中，前文并没有对LOG动作进行示例，此处我们来了解一下LOG动作。

使用LOG动作，可以将符合条件的报文的相关信息记录到日志中，但当前报文具体是被"接受"，还是被"拒绝"，都由后面的规则控制，换句话说，LOG动作只负责记文的相关信息，不负责对报文的其他处理，如果想要对报文进行进一步的处理，可以在之后设置具体规则，进行进一步的处理。

示例如下，下例表示将发往22号端口的报文相关信息记录在日志中。

```
192.168.1.139:22
[www.zsythink.net]#iptables -F
[www.zsythink.net]#iptables -I INPUT -p tcp --dport 22 -j LOG
[www.zsythink.net]#iptables -nvL INPUT
Chain INPUT (policy ACCEPT 14 packets, 1032 bytes)
 pkts bytes target     prot opt in     out     source               destination
   10   720 LOG        tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22 LOG flags 0 lev
[www.zsythink.net]#
[www.zsythink.net]#tail -f /var/log/messages
May  3 13:46:37 testasb kernel: IN=eth4 OUT= MAC=00:0c:29:b7:f4:d1:ac:2b:6e:20:c6:b4:08:00 SRC=192.168.1.88 DST=19
.139 LEN=40 TOS=0x00 PREC=0x00 TTL=64 ID=20532 DF PROTO=TCP SPT=51502 DPT=22 WINDOW=16181 RES=0x00 ACK URGP=0
May  3 13:46:38 testasb kernel: IN=eth4 OUT= MAC=00:0c:29:b7:f4:d1:ac:2b:6e:20:c6:b4:08:00 SRC=192.168.1.88 DST=19
.139 LEN=104 TOS=0x00 PREC=0x00 TTL=64 ID=20555 DF PROTO=TCP SPT=51502 DPT=22 WINDOW=16181 RES=0x00
```


如上图所示，上述规则表示所有发往22号端口的tcp报文都符合条件，所以都会被记录到日志中，查看/var/log/messages即可看到对应报文的相关信息，但是上述示例，因为上例中使用的匹配条件过于宽泛，所以匹配到的报文数量将会非常之多，记录到的信息也不利于分析，所以在使用LOG动作时，匹配条件应该尽量写的精到的报文数量也会大幅度的减少，这样冗余的日志信息就会变少，同时日后分析日志时，日志中的信息可用程度更高。

注：请把刚才用于示例的规则删除。

从刚才的示例中我们已经了解到，LOG动作会将报文的相关信息记录在/var/log/message文件中，当然，我们有可以将相关信息记录在指定的文件中，以防止iptal息与其他日志信息相混淆，修改/etc/rsyslog.conf文件（或者/etc/syslog.conf），在rsyslog配置文件中添加如下配置即可。

#vim /etc/rsyslog.conf

kern.warning /var/log/iptables.log

加入上述配置后，报文的相关信息将会被记录到/var/log/iptables.log文件中。

完成上述配置后，重启rsyslog服务（或者syslogd）

#service rsyslog restart

服务重启后，配置即可生效，匹配到的报文的相关信息将被记录到指定的文件中。

LOG动作也有自己的选项，常用选项如下（先列出概念，后面有示例）

--log-level选项可以指定记录日志的日志级别，可用级别有emerg，alert，crit，error，warning，notice，info，debug。

--log-prefix选项可以给记录到的相关信息添加"标签"之类的信息，以便区分各种记录到的报文信息，方便在分析时进行过滤。

注：--log-prefix对应的值不能超过29个字符。

比如，我想要将主动连接22号端口的报文的相关信息都记录到日志中，并且把这类记录命名为"want-in-from-port-22",则可以使用如下命令

```
[www.zsythink.net]#iptables -F INPUT
[www.zsythink.net]#iptables -I INPUT -p tcp --dport 22 -m state --state NEW -j LOG --log-prefix "want-in-from-port-22"
[www.zsythink.net]#iptables -nL INPUT
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
LOG        tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:22 state NEW LOG flags 0 level 4 prefix `want-in-fron
[www.zsythink.net]#
```


完成上述配置后，我在IP地址为192.168.1.98的客户端机上，尝试使用ssh工具连接上例中的主机，然后查看对应的日志文件（已经将日志文件设置为/var/log/ipta

```
[www.zsythink.net]#cat /var/log/iptables.log
May  4 14:11:35 testasb kernel: want-in-from-port-22IN=eth4 OUT= MAC=00:0c:29:b7:f4:d1:f4:8e:38:82:b1:29
 SRC=192.168.1.98 DST=192.168.1.139 LEN=52 TOS=0x00 PREC=0x00 TTL=128 ID=12929 DF PROTO=TCP SPT=57014 DP
INDOW=8192 RES=0x00 SYN URGP=0
[www.zsythink.net]#
```


如上图所示，ssh连接操作的报文的相关信息已经被记录到了iptables.log日志文件中，而且这条日志中包含"标签"：want-in-from-port-22，如果有很多日志记录过这个"标签"进行筛选了，这样方便我们查看日志，同时，从上述记录中还能够得知报文的源IP与目标IP，源端口与目标端口等信息，从上述日志我们能够看出，19个IP想要在14点11分连接到192.168.1.139（当前主机的IP）的22号端口，报文由eth4网卡进入，eth4网卡的MAC地址为00:0C:29:B7:F4:D1，客户端网卡的mac8-82-B1-29。

除了ACCEPT、DROP、REJECT、LOG等动作，还有一些其他的常用动作，比如DNAT、SNAT等，我们会在之后的文章中对它们进行总结。

希望这篇文章能够对你有所帮助。

iptables 防火墙