** 学习笔记记录，精彩博文收录 **

CasonChan

利用 ipset 封禁大量 IP

使用 iptables 封 IP，是一种比较简单的应对网络攻击的方式，也算是比较常见。有时候可能会封禁成千上万个 IP，如果添加成千上万条规则，在一台注重性能的服务器或者本身性能就很差的设备上，这就是个问题了。ipset 就是为了避免这个问题而生的。

关于 iptables，要知道这两点。

- iptables 包含几个表，每个表由链组成。默认的是 filter 表，最常用的也是 filter 表，另一个比较常用的是 nat 表。一般封 IP 就是在 filter 表的 INPUT 链添加规则。
- 在进行规则匹配时，是从规则列表中从头到尾一条一条进行匹配。

这像是在链表中搜索指定节点费力。ipset 提供了把这个 O(n) 的操作变成 O(1) 的方法：就是把要处理的 IP 放进一个集合，对这个集合设置一条 iptables 规则。像 iptable 一样，IP sets 是 Linux 内核中的东西，ipset 这个命令是对它进行操作的一个工具。

简单的流程

可以用这几条命令概括使用 ipset 和 iptables 进行 IP 封禁的流程

```
ipset create vader hash:ip
iptables -I INPUT -m set --match-set vader src -j DROP
ipset add vader 4.5.6.7
ipset add vader 1.2.3.4
ipset add vader ...
ipset list vader # 查看 vader 集合的内容
```

下面分别对各条命令进行描述。

创建一个集合

```
ipset create vader hash:ip
```

这条命令创建了名为 vader 的集合，以 hash 方式存储，存储内容是 IP 地址。

添加 iptables 规则

```
iptables -I INPUT -m set --match-set vader src -j DROP
```

如果源地址(src)属于 vader 这个集合，就进行 DROP 操作。这条命令中，vader 是作为黑名单的，如果要把某个集合作为白名单，添加一个 '!' 符号就可以。

```
iptables -I INPUT -m set ! --match-set yoda src -j DROP
```

到现在虽然创建了集合，添加了过滤规则，但是现在集合还是空的，需要往集合里加内容。

找出“坏” IP

找出要封禁的 IP，这是封禁过程中重要的步骤，不过不是这里的重点。简要说明一下两种方法思路。

```
netstat -ntu | tail -n +3 | awk '{print $5}' | sort | uniq -c | sort -nr
```

直接通过 netstat 的信息，把与本地相关的各种状态的 IP 都计数，排序列出来。

或者从 nginx 或者其他 web server 的日志里找请求数太多的 IP

```
awk '{print $1}' /var/log/nginx/access.log | sort | uniq -c | sort -nr
```

后半部分，排序，去重，再按次数进行逆向排序的操作，跟上面命令是一样的。

找出“坏” IP，往之前创建的集合里添加就可以了。

```
ipset add vader 4.5.6.7
```


ipset 更多的用法

存储类型

前面例子中的 vader 这个集合是以 hash 方式存储 IP 地址，也就是以 IP 地址为 hash 的键。除了 IP 地址，还可以是网络段，端口号（支持指定 TCP/UDP 协议），mac 地址，网络接口名称，或者上述各种类型的组合。

比如指定 `hash:ip,port`就是 IP 地址和端口号共同作为 hash 的键。查看 ipset 的帮助文档可以看到它支持的所有类型。

下面以两个例子说明。

hash:net

```
ipset create r2d2 hash:net
ipset add r2d2 1.2.3.0/24
ipset add r2d2 1.2.3.0/30 nomatch
ipset add r2d2 6.7.8.9
ipset test r2d2 1.2.3.2
```

`hash:net` 指定了可以往 r2d2 这个集合里添加 IP 段或 IP 地址。

第三条命令里的 `nomatch` 的作用简单来说是把 `1.2.3.0/30` 从 `1.2.3.0/24` 这一范围相对更大的段里“剥离”了出来，也就是说执行完 `ipset add r2d2 1.2.3.0/24` 只后1.2.3.0/24 这一段 IP 是属于 r2d2 集合的，执行了 `ipset add r2d2 1.2.3.0/30 nomatch` 之后，1.2.3.0/24 里 1.2.3.0/30 这部分，就不属于 r2d2 集合了。执行 `ipset test r2d2 1.2.3.2` 就会得到结果 `1.2.3.2 is NOT in set r2d2.`

hash:ip,port

```
ipset create c-3po hash:ip,port
ipset add c-3po 3.4.5.6,80
ipset add c-3po 5.6.7.8,udp:53
ipset add c-3po 1.2.3.4,80-86
```

第二条命令添加的是 IP 地址为 3.4.5.6，端口号是 80 的项。没有注明协议，默认就是 TCP，下面一条命令则是指明了是 UDP 的 53 端口。最后一条命令指明了一个 IP 地址和一个端口号范围，这也是合法的命令。

自动过期，解封

ipset 支持 timeout 参数，这就意味着，如果一个集合是作为黑名单使用，通过 timeout 参数，就可以到期自动从黑名单里删除内容。

```
ipset create obiwan hash:ip timeout 300
ipset add obiwan 1.2.3.4
ipset add obiwan 6.6.6.6 timeout 60
```

上面第一条命令创建了名为 obiwan 的集合，后面多加了 timeout 参数，值为 300，往集合里添加条目的默认 timeout 时间就是 300。第三条命令在向集合添加 IP 时指定了一个不同于默认值的 timeout 值 60，那么这一条就会在 60 秒后自动删除。

隔几秒执行一次 `ipset list obiwan` 可以看到这个集合里条目的 timeout 一直在随着时间变化，标志着它们在多少秒之后会被删除。

如果要重新为某个条目指定 timeout 参数，要使用 `-exit` 这一选项。

```
ipset -exist add obiwan 1.2.3.4 timeout 100
```

这样 `1.2.3.4` 这一条数据的 timeout 值就变成了 100，如果这里设置 300，那么它的 timeout，也就是存活时间又重新变成 300。

如果在创建集合是没有指定 timeout，那么之后添加条目也就不支持 timeout 参数，执行 `add` 会收到报错。想要默认条目不会过期（自动删除），又需要添加某些条目时加上 timeout 参数，可以在创建集合时指定 timeout 为 0。

OpenvSwitch(15)
Python(2)
SDN(6)
Windows(1)
虚拟化(20)

随笔档案

2016年12月(1)
2016年6月(4)
2016年5月(2)
2016年3月(2)
2016年1月(7)
2015年12月(15)
2015年11月(1)
2015年10月(12)
2015年9月(7)
2015年8月(21)
2015年7月(7)
2015年6月(9)
2015年5月(1)
2015年4月(1)
2015年3月(1)
更多

最新评论

1. Re:OpenFlow Switch学习笔记(五)——Group Table、Meter Table及Counters
我想问一下你关于组表的问题，我现在想用带有ovs的四台主机实现负载均衡，所以我想给ovs交换机下组表，结果总是不成功，我想请问一下，组表到底是怎么下的，我是用的手动配置的，我配置进去，但是好像丝毫不起...
--wage

2. Re:UnicodeDecodeError: 'ascii' codec can't decode byte 0xe9 in position 0: ordinal not in range(128) 解决办法
改了后就报错：UnicodeDecodeError: 'utf8' codec can't decode byte 0xb9 in position 1: invalid start byte...
--梁鹊氲@

3. Re:整合Open vSwitch与DNSmasq为虚拟机提供DHCP功能
@ 几米憧憬在宿主机上做下SNAT就可以...
--CasonChan

4. Re:Ubuntu14.04安装配置Open vSwitch
你好，我的open vSwitch是安装在Ubuntu的物理主机上面，但是我一旦将笔记本本地有线端口加入到br0网桥中就不能访问外网了。按你说的dpclient br0后，我的电脑可以通过br0上网，...
--几米憧憬

5. Re:整合Open vSwitch与DNSmasq为虚拟机提供DHCP功能
博主你好，在你这个实验中你能实现虚拟机VM1通过br0桥接通过电脑本地接口eth0上外网吗?
--几米憧憬

阅读排行榜

1. UnicodeDecodeError: 'ascii' codec can't decode byte 0xe9 in position 0: ordinal not in range(128) 解决办法(59948)
2. 利用 ipset 封禁大量 IP(17404)

```
ipset create luke hash:ip
```


更大!

hashsize, maxelem 这两个参数分别指定了创建集合时初始的 hash 大小，和最大存储的条目数量。

```
ipset create yoda hash:ip,port hashsize 4096 maxelem 1000000
ipset add yoda 3.4.5.6,3306
```

这样创建了名为 yoda 的集合，初始 hash 大小是 4096，如果满了，这个 hash 会自动扩容为之前的两倍。最大能存储的数量是 100000 个。

如果没有指定，hashsize 的默认值是 1024，maxelem 的默认值是 65536。

另外几条常用命令

```
ipset del yoda x.x.x.x     # 从 yoda 集合中删除内容
ipset list yoda            # 查看 yoda 集合内容
ipset list                 # 查看所有集合的内容
ipset flush yoda           # 清空 yoda 集合
ipset flush                # 清空所有集合
ipset destroy yoda         # 销毁 yoda 集合
ipset destroy              # 销毁所有集合
ipset save yoda            # 输出 yoda 集合内容到标准输出
ipset save                 # 输出所有集合内容到标准输出
ipset restore              # 根据输入内容恢复集合内容
```

还有……

- 如果创建集合是指定的存储内容包含 ip, 例如 `hash:ip` 或 `hash:ip,port` ，在添加条目时，可以填 IP 段，但是仍然是以单独一个个 IP 的方式来存。
- 上面所有的例子都是用 hash 的方式进行存储，实际上 ipset 还可以以 bitmap 或者 link 方式存储，用这两种方式创建的集合大小，是固定的。
- 通过 `man upset` 和 `ipset –help` 可以查到更多的内容，包括各种选项，支持的类型等等。

转载自https://intxt.net/block-ip-with-ipset/

No pains, no gains

分类: Linux, Network

CasonChan
关注 - 4
粉丝 - 50
+加关注

4 0

« 上一篇： vconfig使用帮助
» 下一篇： 临时解决系统中大量的TIME_WAIT连接

posted on 2016-03-25 14:26 CasonChan 阅读(17405) 评论(0) 编辑 收藏

刷新评论 刷新页面 返回顶部

3. OpenFlow Switch学习笔记(五)——Group Table、Meter Table及Flow Tables(9730)
5. MBR主引导扇区解析(9569)

评论排行榜

1. 整合Open vSwitch与DNSmasq为虚拟机提供DHCP功能(4)
2. Ubuntu14.04安装配置Open vSwitch(2)
3. UnicodeDecodeError: 'ascii' codec can't decode byte 0xe9 in position 0: ordinal not in range(128) 解决办法(1)
4. OpenFlow Switch学习笔记(五)——Group Table、Meter Table及Counters(1)

推荐排行榜

1. 利用 ipset 封禁大量 IP(4)
2. MBR主引导扇区解析(4)
3. 整合Open vSwitch与DNSmasq为虚拟机提供DHCP功能(3)
4. 在KCloud上轻松“玩转”Docker(2)
5. Xen虚拟机磁盘镜像模板制作(三)—CentOS 7(2)

相关博文：
· ipset批量配置iptables
· 如何在Linux下大量屏蔽恶意IP地址
· iptables黑/白名单设置（使用ipset 工具）
· 分享：linux系统如何快速阻止恶意IP地址
· Linuxipnetns命令
» 更多推荐...

最新 IT 新闻:
· 耳朵大战，迫在眉睫
· 网传蔚来包下宁德时代磷酸铁锂电池生产线？官方回应
· OpenAI推DALL-E模型：能根据文字描述生成图片
· NASA新太空望远镜SPHEREx将揭开大爆炸的秘密
· 充不满、掉电快..."怕冷"的磷酸铁锂Model 3如何帮车主们熬过冬天?
» 更多新闻...