iptables防火墙

1. 开启和关闭

启动： service iptables start

重启： service iptables restart

关闭： service iptables stop

2. 配置文件： /etc/sysconfig/iptables

vi /etc/sysconfig/iptables

service iptables restart

/etc/rc.d/init.d/iptables save

3. man iptables

-A：指定链名

-p：指定协议类型

-d：指定目标地址

--dport：指定目标端口

--sport：指定源端口

-j：指定动作类型

4. 不修改配置文件，直接在命令行里敲命令：

添加input记录： iptables -A INPUT -p tcp --dport 22 -j ACCEPT

添加output记录： iptables -A OUTPUT -p tcp --sport 22 -j ACCEPT

/etc/init.d/iptables save：将以上两条语句保存到配置文件/etc/sysconfig/iptables中

5. 给22号端口进行ACCEPT配置

eg：

[root@VerifV5Zbx01 ~]# iptables -L

Chain INPUT (policy ACCEPT)

target	prot opt source	destination	
ACCEPT	all -- anywhere	anywhere	ctstate RELATED,ESTABLISHED
ACCEPT	all -- anywhere	anywhere	
INPUT_direct	all -- anywhere	anywhere	
INPUT_ZONES_SOURCE	all -- anywhere	anywhere	
INPUT_ZONES	all -- anywhere	anywhere	
DROP	all -- anywhere	anywhere	ctstate INVALID
REJECT	all -- anywhere	anywhere	reject-with icmp-host-prohibited

Chain FORWARD (policy DROP)

target	prot opt source	destination	
DOCKER-ISOLATION	all -- anywhere	anywhere	
ACCEPT	all -- anywhere	anywhere	ctstate RELATED,ESTABLISHED
DOCKER	all -- anywhere	anywhere	
ACCEPT	all -- anywhere	anywhere	
ACCEPT	all -- anywhere	anywhere	
ACCEPT	all -- anywhere	anywhere	ctstate RELATED,ESTABLISHED
ACCEPT	all -- anywhere	anywhere	
FORWARD_direct	all -- anywhere	anywhere	
FORWARD_IN_ZONES_SOURCE	all -- anywhere	anywhere	
FORWARD_IN_ZONES	all -- anywhere	anywhere	
FORWARD_OUT_ZONES_SOURCE	all -- anywhere	anywhere	
FORWARD_OUT_ZONES	all -- anywhere	anywhere	
DROP	all -- anywhere	anywhere	ctstate INVALID
REJECT	all -- anywhere	anywhere	reject-with icmp-host-prohibited

Chain OUTPUT (policy ACCEPT)

target	prot opt source	destination
OUTPUT_direct	all -- anywhere	anywhere

```
Chain DOCKER (1 references)
target     prot opt source              destination


Chain DOCKER-ISOLATION (1 references)
target     prot opt source              destination
RETURN     all  --  anywhere            anywhere


Chain FORWARD_IN_ZONES (1 references)
target     prot opt source              destination
FWDI_public  all  --  anywhere            anywhere           [goto]
FWDI_public  all  --  anywhere            anywhere           [goto]


Chain FORWARD_IN_ZONES_SOURCE (1 references)
target     prot opt source              destination


Chain FORWARD_OUT_ZONES (1 references)
target     prot opt source              destination
FWDO_public  all  --  anywhere            anywhere           [goto]
FWDO_public  all  --  anywhere            anywhere           [goto]


Chain FORWARD_OUT_ZONES_SOURCE (1 references)
target     prot opt source              destination


Chain FORWARD_direct (1 references)
target     prot opt source              destination


Chain FWDI_public (2 references)
target     prot opt source              destination
FWDI_public_log  all  --  anywhere            anywhere
FWDI_public_deny  all  --  anywhere            anywhere
FWDI_public_allow  all  --  anywhere            anywhere
ACCEPT     icmp --  anywhere            anywhere


Chain FWDI_public_allow (1 references)
target     prot opt source              destination


Chain FWDI_public_deny (1 references)
target     prot opt source              destination


Chain FWDI_public_log (1 references)
target     prot opt source              destination


Chain FWDO_public (2 references)
target     prot opt source              destination
FWDO_public_log  all  --  anywhere            anywhere
FWDO_public_deny  all  --  anywhere            anywhere
FWDO_public_allow  all  --  anywhere            anywhere


Chain FWDO_public_allow (1 references)
target     prot opt source              destination


Chain FWDO_public_deny (1 references)
target     prot opt source              destination


Chain FWDO_public_log (1 references)
target     prot opt source              destination
```

```
Chain INPUT_ZONES (1 references)
target     prot opt source               destination
IN_public  all  --  anywhere             anywhere            [goto]
IN_public  all  --  anywhere             anywhere            [goto]


Chain INPUT_ZONES_SOURCE (1 references)
target     prot opt source               destination


Chain INPUT_direct (1 references)
target     prot opt source               destination


Chain IN_public (2 references)
target     prot opt source               destination
IN_public_log    all  --  anywhere            anywhere
IN_public_deny   all  --  anywhere            anywhere
IN_public_allow  all  --  anywhere            anywhere
ACCEPT     icmp --  anywhere             anywhere


Chain IN_public_allow (1 references)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:ssh ctstate NEW
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:5666 ctstate NEW
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:http ctstate NEW
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:kerberos ctstate NEW


Chain IN_public_deny (1 references)
target     prot opt source               destination


Chain IN_public_log (1 references)
target     prot opt source               destination


Chain OUTPUT_direct (1 references)
target     prot opt source               destination
[root@VerifV5Zbx01 ~]#
```