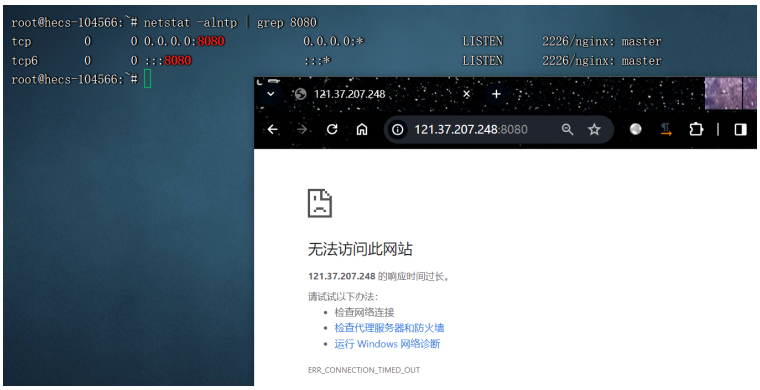
1、配置端口白名单，允许SSH或者特定端口连入服务器：

iptables -A INPUT -p tcp --dport 22 -j ACCEPT

2、将所有其他进入服务器的数据包丢弃：

iptables -A INPUT -j DROP

3、查看本机开放nginx服务，配置完规则后不可以访问：



4、查看本机配置：iptables -L

```
root@hecs-104566:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:10022
ACCEPT     tcp  --  103.85.169.179       anywhere             tcp dpt:http-alt
ACCEPT     tcp  --  39.144.14.159        anywhere             tcp dpt:http-alt
DROP       all  --  anywhere             anywhere
```

查看INPUT规则：iptables -L INPUT

```
root@hecs-104566:~# iptables -L INPUT
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:10022
ACCEPT     tcp  --  103.85.169.179       anywhere             tcp dpt:http-alt
ACCEPT     tcp  --  39.144.14.159        anywhere             tcp dpt:http-alt
ACCEPT     tcp  --  223.104.41.101       anywhere             tcp dpt:http-alt
ACCEPT     tcp  --  223.104.41.100       anywhere             tcp dpt:http-alt
DROP       all  --  anywhere             anywhere
```

5、删除全部iptables配置规则：iptables -F

6、删除单条配置：删除input中的第二条规则：iptables -D INPUT 2

7、添加白名单，可以累加：

iptables -A INPUT -p tcp -s 223.104.41.100 --dport 8080 -j ACCEPT

iptables -A INPUT -p tcp -s 223.104.41.101 --dport 8080 -j ACCEPT

iptables -A INPUT -p tcp -s 223.104.41.102 --dport 8080 -j ACCEPT

```
#! /bin/bash
# 服务器iptables操作脚本
#查看入站配置：  bash iptablesoper.sh show
#删除配置：bash iptablesoper.sh delete 规则行数
#添加配置：bash iptablesoper.sh add IP 端口
case "${1}" in
```

```
  show)
    iptables -L INPUT
  ;;
  delete)
    iptables -D INPUT $2
  ;;
  add)
    iptables -D INPUT -j DROP
    iptables -A INPUT -p tcp -s $2  --dport $3 -j ACCEPT
    iptables -A INPUT -j DROP
esac
```