1. Windows host无法访问centOS虚拟机原因是centOS防火墙
2. CentOS 7.0默认使用的是firewall作为防火墙，这里改为iptables防火墙。  
   firewall：  
   systemctl start firewalld.service#启动firewall  
   systemctl stop firewalld.service#停止firewall  
   systemctl disable firewalld.service#禁止firewall开机启动
3. 安装iptables防火墙

#先检查是否安装了iptablesservice iptables status#安装iptablesyum install -y iptables#升级iptablesyum update iptables #安装iptables-servicesyum install –y iptables-services

1. 设置新的iptables规则

#查看iptables现有规则iptables -L -n#先允许所有,不然有可能会杯具iptables -P INPUT ACCEPT#清空所有默认规则iptables -F#清空所有自定义规则iptables -X#所有计数器归0iptables -Z#允许来自于lo接口的数据包(本地访问)iptables -A INPUT -i lo -j ACCEPT#开放80端口(HTTP)iptables -A INPUT -p tcp --dport 80 -j ACCEPT#允许pingiptables -A INPUT -p icmp --icmp-type 8 -j ACCEPT#允许接受本机请求之后的返回数据 RELATED,是为FTP设置的iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT#其他入站一律丢弃iptables -P INPUT DROP#所有出站一律绿灯iptables -P OUTPUT ACCEPT#所有转发一律丢弃iptables -P FORWARD DROP

#如果要添加内网ip信任（接受其所有TCP请求）iptables -A INPUT -p tcp -s 45.96.174.68 -j ACCEPT#过滤所有非以上规则的请求iptables -P INPUT DROP#要封停一个IP，使用下面这条命令：iptables -I INPUT -s \*\*\*.\*\*\*.\*\*\*.\*\*\* -j DROP#要解封一个IP，使用下面这条命令:iptables -D INPUT -s \*\*\*.\*\*\*.\*\*\*.\*\*\* -j DROP

1. 保存设置

service iptables save

1. 开启iptables服务

#注册iptables服务#相当于以前的chkconfig iptables onsystemctl enable iptables.service#开启服务systemctl start iptables.service#查看状态systemctl status iptables.service

#重启防火墙

service iptables restart

防火墙配置脚本

#!/bin/sh

cd /

iptables -P INPUT ACCEPT

iptables -F

iptables -X

iptables -Z

#iptables -I INPUT -p tcp -j DROP

iptables -A INPUT -i lo -j ACCEPT

iptables -P OUTPUT ACCEPT

#iptables -A INPUT -p tcp --dport 8080 -j ACCEPT

#iptables -I INPUT -s 192.168.2.2 -p tcp --dport 8080 -j ACCEPT

service iptables save

systemctl enable iptables.service

#systemctl start iptables.service

service iptables restart