# Juniper SRX防火墙配置教程1.5

**前言：**

1.蓝色字体表示命令行命令，正式执行时不要复制前面的> # []号，> # []号只是提示符

2.绿色字体表示注释，有时注释太多就不用绿色表示了

3.注意：本文档的所有操作请先在在测环境进行实践，请不要直接在真实的服务器中操作！

**版权声明**：

本文档以开源的形式发布，所有条款如下：

1. 无担保：作者不保证文档内容的准确无误，亦不承担由于使用此文档所导致的任何后果

2. 自由使用：任何人可以出于任何目的而自由地 阅读/链接/打印/转载/引用/再创作 此文档，无需任何附加条件

若您 阅读/链接/打印/转载/引用/再创作 本文档，则说明接受以上2个条款。

作者：李茂福

时间：2022年11月21日

**0.搭建SRX实验环境**

目前还没有可以直接安装运行的Juniper模拟器，官方有vSRX镜像，可以下载并用VirtualBox虚拟机打开，就可用来练习。不过下载官方的镜像要注册一个帐号，比较麻烦。所以在网上找了一份其他大神做好的.ova镜像，读者可自行在网上下载，也可联系作者，**邮箱:** [sysyear@163.com](mailto:sysyear@163.com)

准备事项

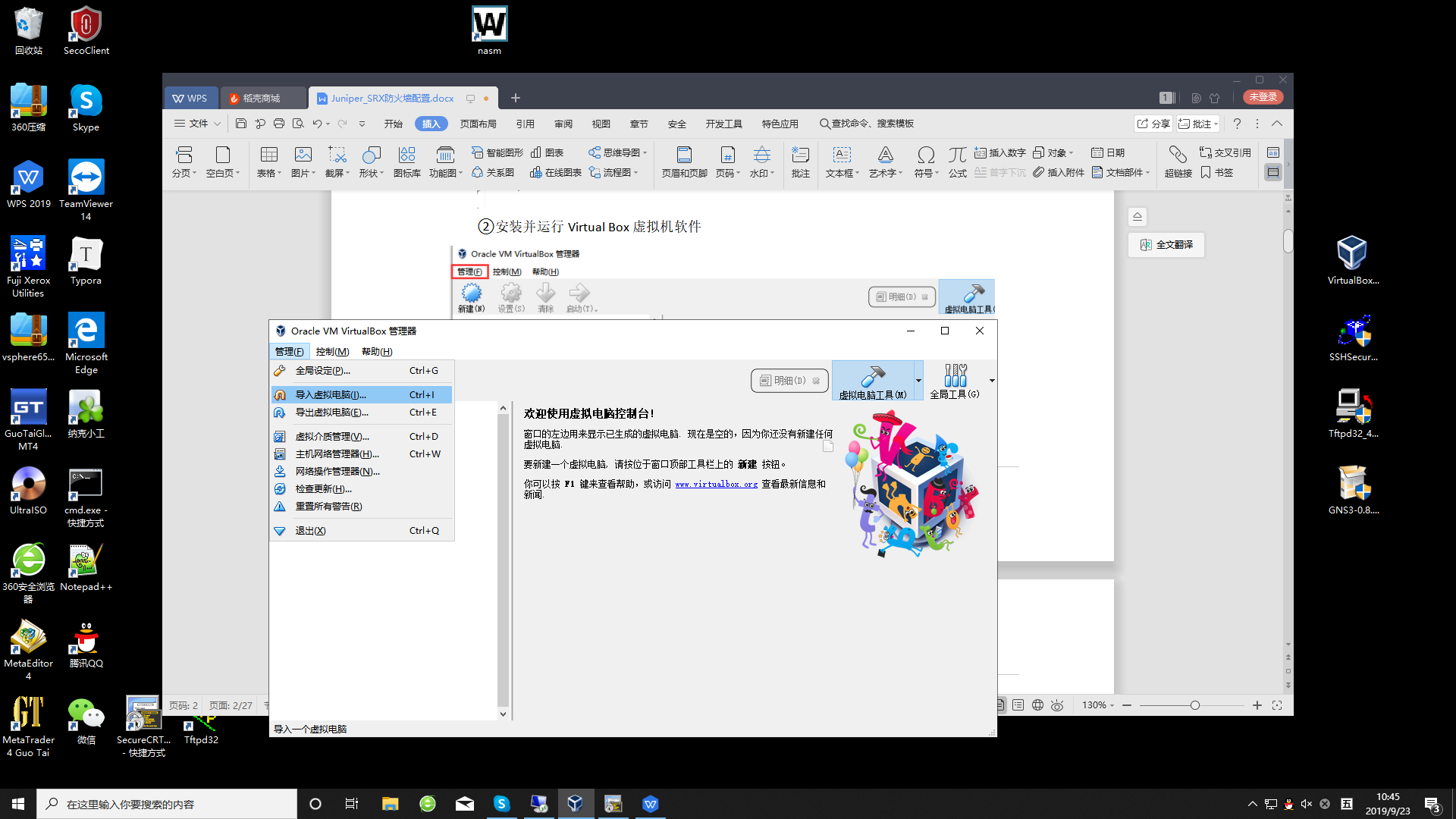
①下载vSRX的.ova文件（本教程使用的是junos-vsrx-12.1X44-D10.4-domestic.ova）到电脑的某个目录下，如D:\Juniper\



②安装并运行Virtual Box虚拟机软件

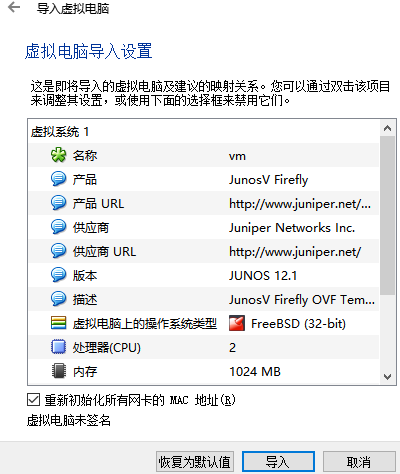


点击主界面左上角的“管理”，“导入虚拟电脑”

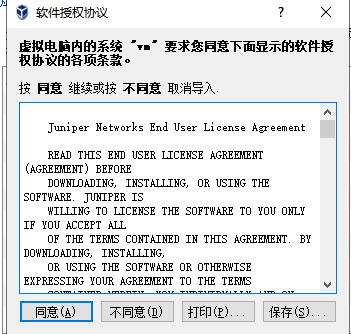


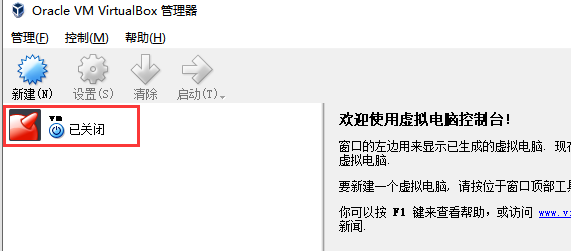
在“导入虚拟电脑”对话框中，选择之前下载的.ova文件，如下图：



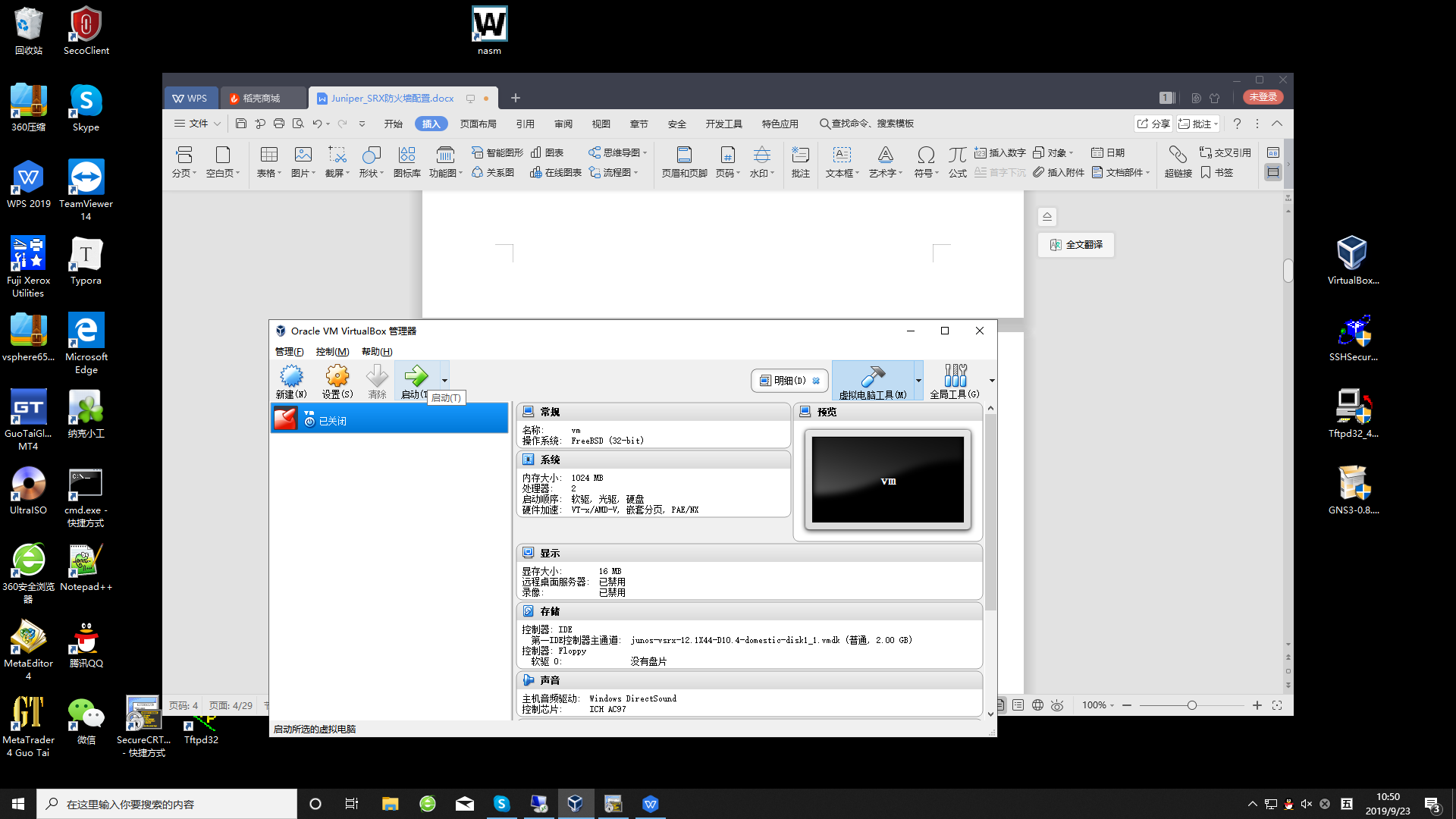


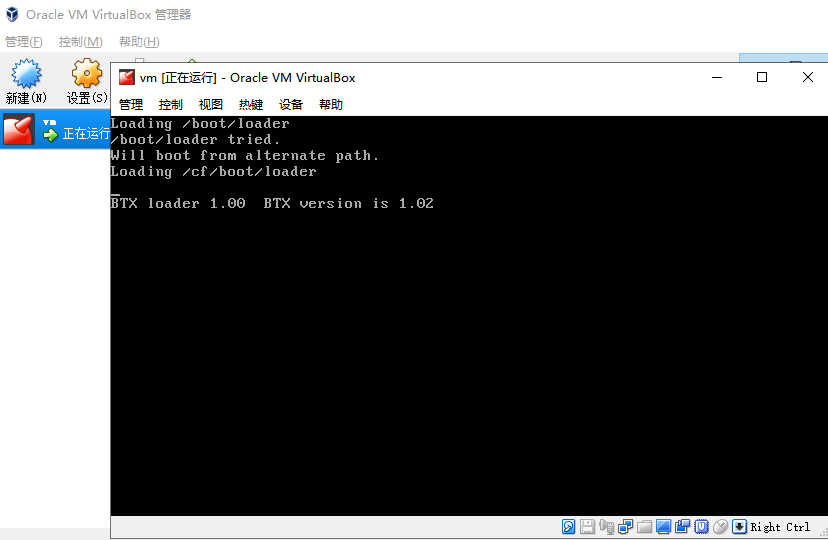
看到了虚拟机的基本配置，点击“导入”，出现下图的软件授权协议，点击“同意”即可





这时虚拟机已添加到VirtualBox里，接下来开启此虚拟机，点击“启动”按钮



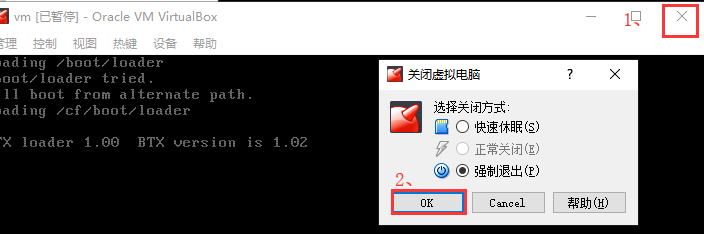


出现上图的界面就说明系统正在启动，需要的时间比较长，大概等待几分钟，，，，

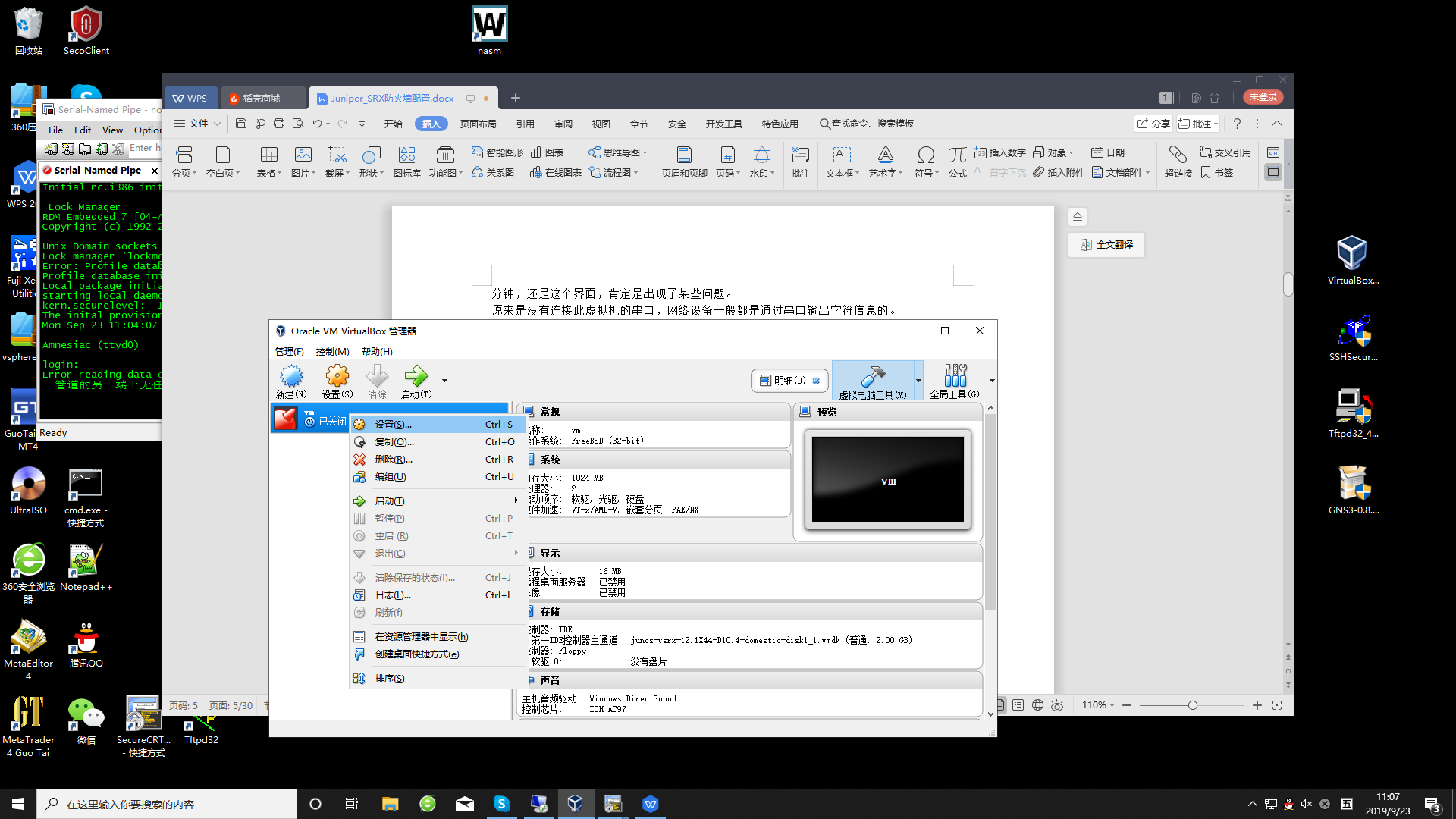
然后不知等了几分钟，还是这个界面，肯定是出现了某些问题。

原来是没有连接此虚拟机的**串口**，网络设备一般都是通过串口输出字符信息的。

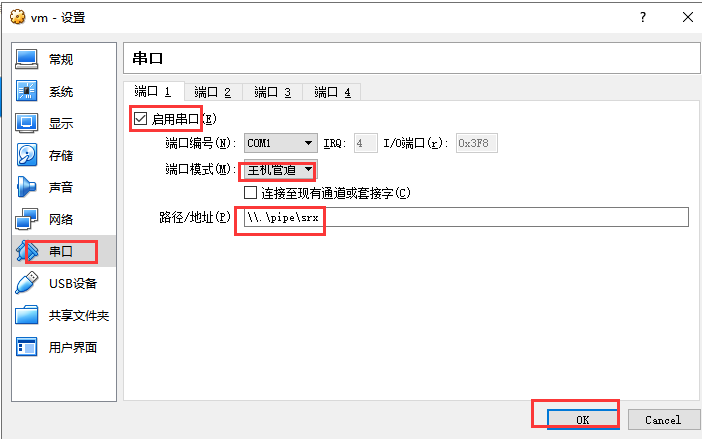
所以，先关机，



再设置此虚拟机



添加串口，设置如下：（记住主机管道的地址，以\\.\pipe\开头，后面的名称自己取一个）



再开机，等待1分半就出现登录界面了



**章n、设备登录管理**

**★初次登录（console登录）**

以root用户登录，初始密码为空，进入系统cli后，再进入配置模式，设置root密码



root@% #最开始进入的是系统底层的命令行，和unix系统差不多

root@% cli #输入 cli 后，回车，进入的才是防火墙的维护与配置界面

root> #提示符为“>”时，表示进入的是防火墙的一般模式

root> configure #在一般模式下输入configure，进入配置模式

root# #提示符为“#”时，表示进入的是防火墙的配置模式

root# set system root-authentication plain-text-password #设置root密码

New password: #输入密码，不回显

Retype new password:

root# commit

commit complete

root# commit #需要两次提交才生效，如果**只提交一次**，默认过2分钟**会回滚**配置

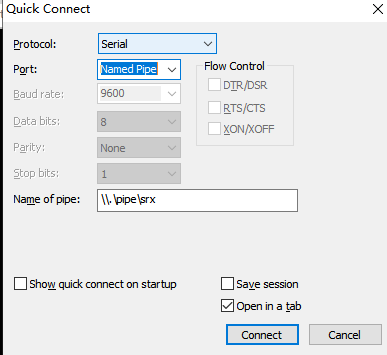
commit complete

root#

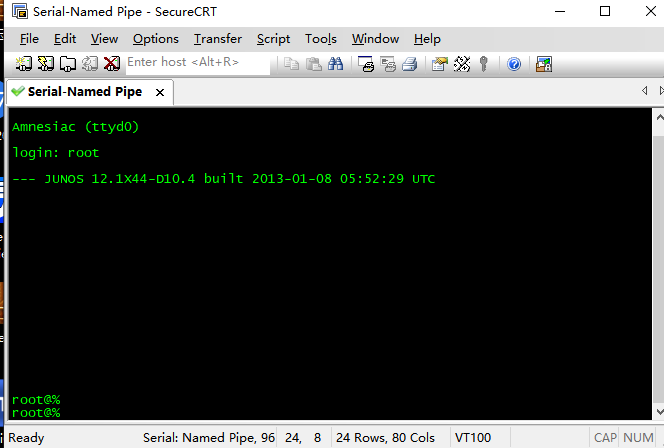
**★连接虚拟机的串口**

在使用虚拟机的过程中，我们发现，VirtualBox自带的console界面不好切换鼠标，也不方便复制粘贴，所以希望使用SecureCRT终端仿真软件连接虚拟机的**串口**，这样也更接近真实的环境，（真实的设备调试也是通过SecureCRT之类的终端仿真软件去连接串口的）

打开SecureCRT，点击快速连接，协议选择Serial，端口为命名管道（Named Pipe）版本在7.0以上的才有。管道名为之前为虚拟机添加的串口里的管道名，以\\.\pipe\开头的，本例中为 \\.\pipe\srx



点击“连接”，就可以了



**★设置系统基本信息（主机名,时区,时间,DNS）**

root# set system host-name SRX550 #设置主机名

[edit]

root@SRX550#

root@SRX550# set system time-zone Asia/Shanghai #设置时区

root@SRX550# run set date 201909201019.00 #手动配置时间

Fri Sep 20 10:19:00 CST 2019

root@Test-SRX# run set date ntp 10.1.1.22 #或者使用ntp

root@Test-SRX# run set date ntp key xxx

root@Test-SRX# run set date ntp source-address 192.168.1.254

**查看时间：**

root@SRX550> show system uptime

**Current time:** **2019-09-20 12:45:35 CST**

System booted: 2019-09-20 10:07:36 CST (02:37:59 ago)

Protocols started: 2019-09-20 10:07:50 CST (02:37:45 ago)

Last configured: 2019-09-20 11:57:28 CST (00:48:07 ago) by root

12:45PM up 2:38, 1 user, load averages: 0.00, 0.00, 0.00

root@SRX550#

root@SRX550# set system name-server 114.114.114.114 #设置DNS，可以设置多行

root@SRX550# commit

commit complete

[edit]

root@SRX550# commit #记得要两次提交，配置才生效

commit complete

root@SRX550> show chassis hardware detail #查看设备详细信息

Hardware inventory:

Item Version Part number **Serial number** Description

**Chassis** AL5216AK0018 SRX550

Midplane REV 22 750-035027 ACPF7615

Routing Engine REV 12 711-035026 ACPM3447 RE-SRXSME-SRX550

ad0 1919 MB ATP COMPACT FLASH 99007160714130200172 Compact Flash

FPC 0 FPC

PIC 0 6x GE, 4x GE SFP Base PIC

Power Supply 0 Rev 04 740-024283 YH52344 PS 645W AC

**★创建用户**

root@SRX550# set system login user coflee class **super-user** authentication plain-text-password #创建一个名为coflee的用户

New password: #输入密码时是不回显的，只管输入

Retype new password: #创建的用户只有加入**super-user**组才有配置设备的权限

[edit]

**★查看登录系统的用户**

root@SRX550> show system users

2:59PM up 4:52, 1 user, load averages: 0.00, 0.00, 0.00

USER TTY FROM LOGIN@ IDLE WHAT

root v0 - Mon02AM - cli

**★设置console输出宽度和行数**

root@SRX550> show cli #查看cli参数

CLI complete-on-space set to on

CLI idle-timeout disabled

CLI restart-on-upgrade set to on

CLI screen-length set to 24 #默认一页显示24行

CLI screen-width set to 80 #默认一行只显示80个字符，超出80个字时会折叠

CLI terminal is 'vt100'

CLI is operating in enhanced mode

CLI timestamp disabled

CLI working directory is '/cf/root'

root@SRX550> set cli screen-width 130 #设置cli界面的屏宽为130个字符

Screen width set to 130

**★查看配置**

root@SRX550> show configuration #在一般模式查看

## Last commit: 2019-09-20 14:50:58 CST by root

version 12.1X44.4;

system {

host-name SRX550;

... ...

root@SRX550# show | display set #以set配置的形式显示配置

... ...

root@SRX550# run show configuration #在配置模式查看

## Last commit: 2019-09-20 14:50:58 CST by root

version 12.1X44.4;

system {

host-name SRX550;

... ...

**★基本维护查看命令**

root@SRX550> show system users #查看系统目前登录的用户

12:01PM up 1:54, 1 user, load averages: 0.00, 0.00, 0.00

USER TTY FROM LOGIN@ IDLE WHAT

root d0 - Mon02AM - cli

root@SRX550> show system software #查看系统软件版本

Information for junos:

Comment:

JUNOS Software Release [12.1X44-D10.4]

root@SRX550> show system uptime #查看当前时间及开机时间

Current time: 2019-09-20 12:01:41 CST

System booted: 2019-09-20 10:07:36 CST (01:54:05 ago)

Protocols started: 2019-09-20 10:07:50 CST (01:53:51 ago)

Last configured: 2019-09-20 11:57:28 CST (00:04:13 ago) by root

12:01PM up 1:54, 1 user, load averages: 0.00, 0.00, 0.00

root@SRX550> show chassis environment

Class Item Status Measurement

Temp Routing Engine Testing

Routing Engine CPU Absent

Power Power Supply 0 OK

root@SRX550> show chassis hardware

Hardware inventory:

Item Version Part number Serial number Description

Chassis AL5216AK0018 SRX550

Midplane REV 22 750-035027 ACPF7615

Routing Engine REV 12 711-035026 ACPM3447 RE-SRXSME-SRX550

FPC 0 FPC

PIC 0 6x GE, 4x GE SFP Base PIC

Power Supply 0 Rev 04 740-024283 YH52344 PS 645W AC

root@SRX550> show chassis firmware

Part Type Version

FPC 0 O/S Version 12.1X46-D35.1 by builder on 2015-05

FWDD O/S Version 12.1X46-D35.1 by builder on 2015-05

root@SRX550> show chassis routing-engine

Routing Engine status:

Total memory 1024 MB Max 532 MB used ( 52 percent)

Control plane memory 594 MB Max 315 MB used ( 53 percent)

Data plane memory 430 MB Max 215 MB used ( 50 percent)

CPU utilization:

User 0 percent

Background 0 percent

Kernel 0 percent

Interrupt 0 percent

Idle 100 percent

Model JUNOSV-FIREFLY RE

Start time 2019-09-23 02:42:43 CST

Uptime 1 hour, 56 minutes, 42 seconds

Last reboot reason Router rebooted after a normal shutdown.

Load averages: 1 minute 5 minute 15 minute

0.00 0.00 0.00

root> show route #查看路由表

root> show arp #查看arp表

root> show interface terse #查看端口状态及IP

root> show log

root> ping 192.168.1.1 count 3 #icmp测试

root@SRX550> show log messages

Sep 20 09:13:26 eventd[936]: SYSTEM\_ABNORMAL\_SHUTDOWN: System abnormally shut down

Sep 20 09:13:26 eventd[936]: SYSTEM\_OPERATIONAL: System is operational

Sep 20 09:13:26 /kernel: Copyright (c) 1996-2013, Juniper Networks, Inc.

Sep 20 09:13:26 /kernel: All rights reserved.

Sep 20 09:13:26 /kernel: Copyright (c) 1992-2006 The FreeBSD Project.

Sep 20 09:13:26 /kernel: Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994

Sep 20 09:13:26 /kernel: The Regents of the University of California. All rights reserved.

**★删除某条配置**

root@SRX550# delete interfaces ge-0/0/0.0 family inet address 192.168.0.200/24

root@SRX550# delete security zones security-zone trust interfaces ge-0/0/1.0

如何该条配置不存在会有提示：

warning: statement not found

#设置时使用set，删除某条设置时使用delete，后边的都一样

**★保存系统配置**

root@SRX550**#** save conf.cfg #保存的文件名为 conf.cfg，在配置模式下保存

Wrote 330 lines of configuration to 'conf.cfg'

root@SRX550**>** file list #查看当前登录用户的家目前下的文件

/cf/root/:

.cshrc

.history

.login

.profile

**conf.cfg**

xxx.cfg

**★以配置文件恢复现在运行的设置**

root@SRX550# load override conf.cfg

load complete

root@SRX550# load override ftp:#user:passwd@10.1.1.1/filename.cfg

root@SRX550# commit

commit complete

[edit]

root@SRX550# commit #记得要两次提交

commit complete

**★FTP备份/下载文件**

root@SRX550> file copy conf.cfg ftp:#user:passwd@10.1.1.1/filename.cfg

#复制文件至ftp服务器上，格式为ftp:#ftp用户:密码@服务器ip/目标文件名

**★恢复出厂设置**

root@SRX550# load factory-default

warning: activating factory configuration

#恢复出厂后，要设置root用户密码，再两次提交，保存配置，重启系统

root# set system root-authentication plain-text-password #设置root密码

New password: #输入密码，不回显

Retype new password:

root# commit

commit complete

root# commit #需要两次提交才生效，如果**只提交一次**，默认过2分钟**会回滚**配置

commit complete

root#

**★设备停机、重启**

root@Test-SRX> request system halt #停机

Halt the system ? [yes,no] (no) yes

syncing disks... All buffers synced.

Uptime: 5h15m47s

Normal shutdown (no dump device defined)

The operating system has halted.

Please press any key to reboot. #在停机状态下若按下任意一个键，系统都会重启

root@SRX550> request system reboot #重启系统

System going down IMMEDIATELY

**★配置回滚设置**

root@SRX550# set system max-configurations-on-flash 5

#设置系统保存配置的副本数（用以回滚的配置）

root@SRX550# set system max-configurations-rollbacks 5

root@SRX550# commit confirmed 2 #设置回滚的时间，2分钟后若无第二次提交则回滚

commit confirmed will be automatically rolled back in 2 minutes unless confirmed

commit complete

# commit confirmed will be rolled back in 2 minutes

[edit]

root@SRX550#

root@SRX550# commit check #提交配置前先检查一下配置的语法

configuration check succeeds

root@SRX550# rollback ?

Possible completions:

<[Enter]> Execute this command

0 2019-09-20 11:53:30 CST by root via cli

1 2019-09-20 11:53:28 CST by root via cli

2 2019-09-20 11:53:12 CST by root via cli commit confirmed, rollback in 2mins

3 2019-09-20 11:47:17 CST by root via cli

4 2019-09-20 11:47:16 CST by root via cli

5 2019-09-20 11:19:06 CST by root via cli

6 2019-09-20 11:19:05 CST by root via cli

7 2019-09-20 11:10:58 CST by root via cli

8 2019-09-20 11:10:57 CST by root via cli

root@SRX550# rollback 1 #回滚到系统保留的1号配置

load complete

[edit]

**★CLI界面升级系统**

root@Test-SRX> file copy ftp:#user:passwd@10.1.1.1/junos-xxx.tgz junos2.tgz

root@Test-SRX> request system software add junos2.tgz no-validate reboot

**★boot模式**

**★boot模式下升级系统**

#重启或开机时出现如下行时按下空格，进入boot模式

Hit [Enter] to boot immediately, or space bar for command prompt.

Type '?' for a list of commands, 'help' for more detailed help.

**OK** #boot模式下的提示符为 OK

OK

OK ? #输入问号，按下回车 可以查看支持的命令

Available commands:

reboot reboot the system

boot boot a file or loaded kernel

set set a variable

unset unset a variable

nextboot set next boot device

install install JUNOS

ls list files

recover initiate recovery process from compact flash

boot-conf load kernel and modules, then autoboot

......

OK

OK show #输入show查看全局环境设置

LINES=24

autoboot\_delay=2

boot.status=0xa0002

boot\_serial=YES

bootfile=/kernel;/kernel.old

comconsole\_speed=9600

console=comconsole

currdev=disk1s1a:

......

#设置ip和tftp服务器ip

OK set ipaddr=10.1.1.1

OK set serverip=10.1.1.2

OK set netmask=255.255.255.0

OK install tftp:#10.1.1.2/junos-xxx.tgz #安装系统，以eth0为管理接口

**★恢复密码，原配置不变**

#重启或开机时出现如下行时按下空格，进入boot模式，提示符为 OK

Hit [Enter] to boot immediately, or space bar for command prompt.

OK boot -s #进入单用户模式

.......

Enter full pathname of shell or 'recovery' for root pwd recovery or RETURN for /bin/sh: recovery

#这里输入 recovery

.......

Starting CLI ...

root@Test-SRX>

root@Test-SRX> configure #进入配置模式

root@Test-SRX# delete system root-authentication #先删除root密码

root@Test-SRX# set system root-authentication plain-text-password #重新设置

New password: #输入密码，不回显

Retype new password: #再次输入密码

[edit]

root@Test-SRX# commit

root@Test-SRX# commit #需要2次提交才生效

commit complete

root@Test-SRX# save config2.cfg #记得备份配置 ???

Wrote 330 lines of configuration to 'config2.cfg'

[edit]

root@Test-SRX# exit

root@Test-SRX> request system reboot #重启系统，进入正常的模式

Reboot the system ? [yes,no] (no) yes

Shutdown NOW!

[pid 1364]

重启后以root用户登录，输入刚刚设置的密码即可

login: root

Password:

--- JUNOS 12.1X46-D35.1 built 2015-05-14 23:19:08 UTC

**★开启远程登录服务**

root@SRX550# set system services telnet

[edit]

root@SRX550# set system services ssh

[edit]

root@SRX550# set system services web-management https

root@SRX550# set system services ssh root-login ? #按下？问号也是有提示的

Possible completions:

allow Allow root access via ssh

deny Do not allow root access via ssh

deny-password Allow for non-password-based authentication methods only

[edit]

root@SRX550# set system services ssh root-login deny #禁止root用户登录

root@SRX550# set system services telnet connection-limit 5 #限制连接数

root@SRX550# set system services web-management https system-generated-certificate

root@SRX550# set system services web-management https interface ge-0/0/0.0

#指定允许登录web的接口

root@SRX550# set system services web-management https interface ge-0/0/0.0 port 8899 #指定登录web的端口号

root@SRX550# set system services web-management session idle-timeout ?

Possible completions:

<idle-timeout> Default timeout of web-management sessions (minutes)

root@SRX550# set system services web-management session idle-timeout 20

#登录空闲超时，单位：分钟，web无操作20分钟即断开连接

#开启远程登录服务后，要放行该服务的流量，即允许该服务流量进入防火墙的管理端口

**★重启web服务**

root@SRX550> restart web-management

Web management gatekeeper process started, pid 3833

#如果http/https无法登录或无响应，可以重启该服务

**章n、端口/接口操作**

**★接口安全域操作**

**★查看安全域绑定的接口**

root@SRX550> show security zones

Security zone: trust

Send reset for non-SYN session TCP packets: Off

Policy configurable: Yes

Interfaces bound: 1

Interfaces:

vlan.0

Security zone: untrust

Send reset for non-SYN session TCP packets: Off

Policy configurable: Yes

Screen: untrust-screen

Interfaces bound: 1

Interfaces:

ge-0/0/0.0

Security zone: junos-host

Send reset for non-SYN session TCP packets: Off

Policy configurable: Yes

Interfaces bound: 0

Interfaces:

........

**★接口加入安全域**

root@SRX550# set security zones security-zone trust interfaces ge-0/0/0.0

root@SRX550# set security zones security-zone untrust interfaces ge-0/0/1.0

**★管理口放行服务**

root@SRX550# set security zones security-zone trust interfaces ge-0/0/1.0 host-inbound-traffic system-services all #放行所有入站流量

root@SRX550# set security zones security-zone untrust interfaces ge-0/0/2.0 host-inbound-traffic system-services ping #只放行具体的某种报文，如icmp

root@SRX550# set security zones security-zone untrust interfaces ge-0/0/2.0 host-inbound-traffic system-services telnet

root@SRX550# set security zones security-zone untrust interfaces ge-0/0/2.0 host-inbound-traffic system-services ssh

root@SRX550# set security zones security-zone untrust interfaces ge-0/0/2.0 host-inbound-traffic system-services https

**★放通安全域之间的流量**

root@SRX550# set security policies from-zone trust to-zone untrust policy

trust\_to\_untrust match source-address any destination-address any

root@SRX550# set security policies from-zone trust to-zone untrust policy trust\_to\_untrust then permit

#创建一条安全策略，名为trust\_to\_untrust，动作为permit

from-zone untrust to-zone trust { #系统有一条从untrust到trust的默认策略是deny

policy default-deny {

match {

source-address any;

destination-address any;

application any;

}

then {

**deny;**

}

}

}

**★接口配置IP**

root@SRX550# set interfaces ge-0/0/0 unit 0 family inet address 192.168.1.254/24

[edit]

root@SRX550# set interfaces ge-0/0/1.0 family inet address 200.1.1.2/24

# 2种子接口配置方式，默认不会覆盖原有ip配置，只会叠加，一个子接口可用多个ip

**★查看接口IP及link状态**

root@SRX550> show interfaces terse

Interface Admin Link Proto Local Remote

ge-0/0/0 up up

ge-0/0/0.0 up up inet 192.168.1.254/24

lt-0/0/0 up up

mt-0/0/0 up up

sp-0/0/0 up up

sp-0/0/0.0 up up inet

sp-0/0/0.16383 up up inet 10.0.0.1 --> 10.0.0.16

10.0.0.6 --> 0/0

128.0.0.1 --> 128.0.1.16

128.0.0.6 --> 0/0

ge-0/0/1 up up

ge-0/0/1.0 up up inet 200.1.1.2/24

ge-0/0/3 up up

ge-0/0/3.0 up up eth-switch

dsc up up

vlan up up

vlan.0 up up inet 192.168.1.1/24

**章n、路由配置**

**★静态路由**

root@SRX550# set routing-options static route 0.0.0.0/0 next-hop 200.1.1.22

root@SRX550> show route

inet.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)

+ = Active Route, - = Last Active, \* = Both

0.0.0.0/0 \*[Static/5] 00:00:04

> to 200.1.1.22 via ge-0/0/1.0

192.168.1.0/24 \*[Direct/0] 00:41:27

> via ge-0/0/0.0

192.168.1.254/32 \*[Local/0] 00:41:27

Local via ge-0/0/0.0

200.1.1.0/24 \*[Direct/0] 00:41:27

> via ge-0/0/1.0

200.1.1.2/32 \*[Local/0] 00:41:27

Local via ge-0/0/1.0

**章n、NAT地址转换**

**14.源NAT**

root@SRX550# set security nat source rule-set toInternet from zone trust

root@SRX550# set security nat source rule-set toInternet to zone untrust

root@SRX550# set security nat source rule-set toInternet rule r1 match source-address 0.0.0.0/0 destination-address 0.0.0.0/0

root@SRX550# set security nat source rule-set toInternet rule r1 then source-nat interface

**★目的NAT（端口映射）**

root@SRX550# set security nat destination pool towebser address 192.168.1.10 port 80 #内网IP及端口号

root@SRX550# set security nat destination rule-set r\_towebser from zone untrust

root@SRX550# set security nat destination rule-set r\_towebser rule r1 match source-address 0.0.0.0/0 #匹配外网的源ip

root@SRX550# set security nat destination rule-set r\_towebser rule r1 match destination-address 200.1.1.2/32 #用于端口映射的外网口IP

root@SRX550# set security nat destination rule-set r\_towebser rule r1 match destination-port 2333 #外网端口号

root@SRX550# set security nat destination rule-set r\_towebser rule r1 then destination-nat pool towebser

**放行该端口的策略**

root@SRX550# set applications application tcp\_80 protocol tcp destination-port 80

#内网端口号，因为外部报文进来时已经做了端口转换了

root@SRX550# set security zones security-zone trust address-book address ab\_192.168.1.10 192.168.1.10/32 #内网的IP

root@SRX550# set security policies from-zone untrust to-zone trust policy p\_towebser match source-address any

root@SRX550# set security policies from-zone untrust to-zone trust policy p\_towebser match destination-address ab\_192.168.1.10

root@SRX550# set security policies from-zone untrust to-zone trust policy p\_towebser match application tcp\_80

root@SRX550# set security policies from-zone untrust to-zone trust policy p\_towebser then permit [application-services utm-policy default-av]

**★ARP代理**

**当一个接口上有多个IP要使用时，要做arp代理**

root@SRX550# set security nat proxy-arp interface ge-0/0/1.0 address 200.1.1.3 to 200.1.1.9

**19.查看防火墙会话数**

root@SRX550> show security flow session summary

Unicast-sessions: 2

Multicast-sessions: 0

Failed-sessions: 0

Sessions-in-use: 2

Valid sessions: 2

Pending sessions: 0

Invalidated sessions: 0

Sessions in other states: 0

Maximum-sessions: 131072

**查找指定端口会话数**

root@SRX550> show security flow session destination-port 22

**清除指定会话**

root@SRX550> clear security flow session session-identifier 44321(ID)

#当该端口的服务被占满时，比如系统只允许5个ssh会话，结果管理人员登录后没有退出，占满了这5个会话数，就不能再用ssh登录了，这时可以用telnet登录，或者用console登录，再使用上面的命令清除无用的ssh会话

**20.pppoe拨号设置**

root@SRX550# set interfaces ge-0/0/0 unit 0 encapsulation ppp-over-ether

#要拨号的接口

root@SRX550# set interfaces pp0 unit 0 pppoe-options underlying-interface

ge0/0/0 auto-reconnect 100 idle-timeout 100 client

root@SRX550# set interfaces pp0 unit 0 family inet mtu 1492

root@SRX550# set interfaces pp0 unit 0 family inet negotiate-address

root@SRX550# set interfaces pp0 unit 0 ppp-options pap default-password

123456xx local-name cofxx local-password 123456xx passive

或者

root@SRX550# set interfaces pp0 unit 0 ppp-options chap

default-chap-secret 123456xx local-name cofxx passive

root@SRX550# set routing-options static route 0.0.0.0/0 next-hop pp0.0

查看pppoe

> show pppoe interface

> show pppoe version

> show pppoe statistics

**21.Dynamic VPN 设置**

**A：配置vpn接入认证模板，接入地址池设置**

root@SRX550# set access profile dvpn\_acc\_profile client coflee

firewall-user password 123456xx

root@SRX550# set access profile dvpn\_acc\_profile address-assignment

pool dvpn\_addr\_pool

root@SRX550# set access address-assignment pool dvpn\_addr\_pool family inet

network 192.168.200.0/24

root@SRX550# set access address-assignment pool dvpn\_addr\_pool family

inet xauth-attributes primary-dns 114.114.114.114

root@SRX550# set access firewall-authentication web-authentication

default-profile dvpn\_acc\_profile

**B：配置ike proposal**

root@SRX550# set security ike proposal ike\_pro authentication-method

pre-shared-keys

root@SRX550# set security ike proposal ike\_pro dh-group group2

root@SRX550# set security ike proposal ike\_pro authentication-algorithm sha1

root@SRX550# set security ike proposal ike\_pro encryption-algorithm aes-128-cbc

root@SRX550# set security ike proposal ike\_pro lifetime-seconds 36000

#180至86400

**C：配置第一阶段的ike**

root@SRX550# set security ike policy ike\_policy mode aggressive

root@SRX550# set security ike policy ike\_policy proposal-set ike\_pro

#proposal-set可自定义，也可用系统预设的,如standard

root@SRX550# set security ike policy ike\_policy pre-shared-key ascii-text pre123455

root@SRX550# set security ike gateway ike\_gateway ike-policy ike\_policy

root@SRX550# set security ike gateway ike\_gateway dynamic hostname srx550

root@SRX550# set security ike gateway ike\_gateway dynamic connections-limit 10

root@SRX550# set security ike gateway ike\_gateway dynamic

ike-user-type group-ike-id

root@SRX550# set security ike gateway ike\_gateway external-interface ge-0/0/1

root@SRX550# set security ike gateway ike\_gateway xauth

access-profile dvpn\_acc\_profile

**D：配置ipsec proposal**

root@SRX550# set security ipsec proposal ipsec\_pro protocol esp

root@SRX550# set security ipsec proposal ipsec\_pro

authentication-algorithm hmac-sha1-96

root@SRX550# set security ipsec proposal ipsec\_pro encryption-algorithm 3des-cbc

root@SRX550# set security ipsec proposal ipsec\_pro lifetime-seconds 36000

#180~86400

root@SRX550# set security ipsec proposal ipsec\_pro lifetime-kilobytes 500000 #(64..4294967294 kilobytes)

**E：配置第二阶段的ipsec及vpn**

root@SRX550# set security ipsec policy ipsec\_policy proposal-set ipsec\_pro

#proposal-set可自定义，也可用系统预设的,如standard

root@SRX550# set security ipsec vpn dyn\_vpn ike gateway ike\_gateway

root@SRX550# set security ipsec vpn dyn\_vpn ike ipsec-policy ipsec\_policy

**F：配置dvpn**

root@SRX550# set security dynamic-vpn access-profile dvpn\_acc\_profile

root@SRX550# set security dynamic-vpn clients c\_group1

remote-protected-resources 192.168.1.0/24

root@SRX550# set security dynamic-vpn clients c\_group1 remote-exceptions 0.0.0.0/0 #其余的不走vpn

root@SRX550# set security dynamic-vpn clients c\_group1 ipsec-vpn dyn\_vpn

root@SRX550# set security dynamic-vpn clients c\_group1 user coflee

**G：放行流量 策略**

root@SRX550# set security policies from-zone untrust to-zone trust policy

to\_vpn match source-address any

root@SRX550# set security policies from-zone untrust to-zone trust policy

to\_vpn match destination-address any

root@SRX550# set security policies from-zone untrust to-zone trust policy

to\_vpn match application any

root@SRX550# set security policies from-zone untrust to-zone trust policy

to\_vpn then permit tunnel ipsec-vpn dyn\_vpn

root@SRX550# set security zones security-zone untrust interfaces

ge0/0/1 host-inbound-traffic system-services ike

**查看vpn**

root@SRX550> show security dynamic-vpn users

root@SRX550> show security ike security-associations

root@SRX550> show security ipsec security-associations

Total active tunnels: 0

**22.IPsec VPN (站到站)**

使用默认的安全隧道接口st0，类似于gre over ipsec，基于路由的ipsec vpn

A：设置隧道接口，创建保护流

root@SRX550# set interfaces st0 unit 0 family inet address 10.1.1.1/24

root@SRX550# set security zones security-zone untrust interfaces st0.0

root@SRX550# set routing-options static route 192.168.200.0/24 next-hop st0.0

B：配置ike

root@SRX550# set security ike policy ike\_policy mode main

root@SRX550# set security ike policy ike\_policy proposal-set standard

root@SRX550# set security ike policy ike\_policy pre-shared-key ascii-text 123456xx

root@SRX550# set security ike policy ike\_policy pre-shared-key ascii-text 123456xx

root@SRX550# set security ike gateway gw1 ike-policy ike\_policy

root@SRX550# set security ike gateway gw1 external-interface ge-0/0/0.0

C：配置ipsec

root@SRX550# set security ipsec policy ipsec\_policy proposal-set standard

root@SRX550# set security ipsec vpn vpn\_1 bind-interface st0.0

root@SRX550# set security ipsec vpn vpn\_1 ike gateway gw1

root@SRX550# set security ipsec vpn vpn\_1 ike ipsec-policy ipsec\_policy

root@SRX550# set security ipsec vpn vpn\_1 establish-tunnels immediately

D：放行vpn流量

root@SRX550# set security policies from-zone untrust to-zone trust policy

to\_vpn match source-address 192.168.100.0/24 #对端的内网ip

root@SRX550# set security policies from-zone untrust to-zone trust policy

to\_vpn match destination-address any

root@SRX550# set security policies from-zone untrust to-zone trust policy

to\_vpn match application any

root@SRX550# set security policies from-zone untrust to-zone trust policy

to\_vpn then permit

root@SRX550# set security zones security-zone untrust interfaces

ge-0/0/0.0 host-inbound-traffic system-services ike

**23.策略路由FBF**

**也叫 FBF（Filter-Based Forwarding）**

**A：创建路由实例**

root@Test-SRX# set routing-instances ri\_1 instance-type forwarding

root@Test-SRX# set routing-instances ri\_1 routing-options static route

0.0.0.0/0 next-hop pp0.0

**B：设置防火墙过滤**

root@Test-SRX# set firewall filter to\_dx term 1 from source-address 192.168.20.0/24

root@Test-SRX# set firewall filter to\_dx term 1 then routing-instance ri\_1

root@Test-SRX# set interfaces ge-0/0/0 unit 0 family inet filter input to\_dx

#应用到内网口上

**24.SNMP**

root@SRX550# set snmp location "zhongguo"

root@SRX550# set snmp contact "xxx@x.com"

root@SRX550# set snmp community pub123456 authorization read-write

root@SRX550# set snmp community pub123456 clients 10.1.1.0/24

root@SRX550# set snmp trap-group tra123456 version v2

root@SRX550# set snmp trap-group tra123456 categories authentication

root@SRX550# set snmp trap-group tra123456 categories link

root@SRX550# set snmp trap-group tra123456 categories remote-operations

root@SRX550# set snmp trap-group tra123456 categories routing

root@SRX550# set snmp trap-group tra123456 categories configuration

root@SRX550# set snmp trap-group tra123456 targets 10.1.1.22

root@SRX550# set security zones security-zone trust interfaces

ge-0/0/0.0 host-inbound-traffic system-services snmp

**32. VRRP**

root@SRX-02# set interfaces ge-0/0/0.0 family inet address 192.168.0.152/24

vrrp-group 1 virtual-address 192.168.0.254 #vrrp组为1,虚拟网关为~0.254

root@SRX-02# set interfaces ge-0/0/0.0 family inet address 192.168.0.152/24 vrrp-group 1 priority 120 #优先级为120,默认为100,越大越优先

root@SRX-02# set interfaces ge-0/0/0.0 family inet address 192.168.0.152/24 vrrp-group 1 accept-data #允许虚拟网关接收icmp报文等数据

root@SRX-02# set interfaces ge-0/0/0.0 family inet address 192.168.0.152/24 vrrp-group 1 preempt #抢占模式，no-preempt为 非抢占

root@SRX-02# set interfaces ge-0/0/0.0 family inet address 192.168.0.152/24 vrrp-group 1 advertise-interval 2 #秒，报文通告周期，默认为1秒

root@SRX-02# set interfaces ge-0/0/0.0 family inet address 192.168.0.152/24 vrrp-group 1 advertisements-threshold 3 #达到3次收不到对端的报文就认为对端已经不在线了

root@SRX-02# set interfaces ge-0/0/0.0 family inet address 192.168.0.152/24 vrrp-group 1 authentication-type md5 #备份组成员之间的验证方式为md5

root@SRX-02# set interfaces ge-0/0/0.0 family inet address 192.168.0.152/24 vrrp-group 1 authentication-key 123456xx #验证密码

root@SRX-02# set interfaces ge-0/0/0.0 family inet address 192.168.0.152/24 vrrp-group 1 track interface ge-0/0/1.0 priority-cost 30 #track

**\*放行vrrp入站流量**

root@SRX-02# set security zones security-zone untrust interfaces ge-0/0/0.0 host-inbound-traffic protocols vrrp

root@SRX-02# set security zones security-zone untrust interfaces ge-0/0/0.0 host-inbound-traffic system-services ping

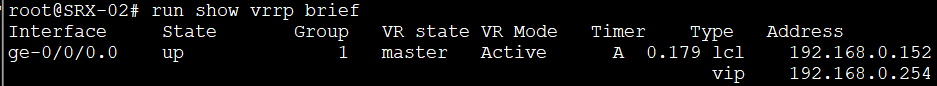
root@SRX-02# commit #提交配置，使配置生效

commit complete

root@SRX-02# commit

commit complete

root@SRX-02# run show vrrp brief #查看vrrp基本情况



root@SRX-02# run show vrrp track #查看track监控状况

**33. DHCP**

root@SRX-02# set system services dhcp pool 10.2.2.0/24 address-range

low 10.2.2.100 #地址池10.2.2.0/24,起始地址10.2.2.100

root@SRX-02# set system services dhcp pool 10.2.2.0/24 address-range

high 10.2.2.200 #结束地址10.2.2.200

root@SRX-02# set system services dhcp pool 10.2.2.0/24 maximum-lease-time 42000

#最大租期42000秒

root@SRX-02# set system services dhcp pool 10.2.2.0/24 default-lease-time 36000

#默认分配的租期36000秒，不能大于最大租期

root@SRX-02# set system services dhcp pool 10.2.2.0/24 name-server 8.8.8.8

#分配给客户端的DNS服务器IP，可以分配多个，一条命令设置一个

root@SRX-02# set system services dhcp pool 10.2.2.0/24 router 10.2.2.254

#默认网关

root@SRX-02# set security zones security-zone trust interfaces ge-0/0/1.0 host-inbound-traffic system-services dhcp #放行dhcp入站流量

root@SRX-02# run show system services dhcp binding #查看IP分配情况

IP address Hardware address Type Lease expires at

10.2.2.100 00:50:56:c0:00:01 dynamic 2020-01-22 12:53:41 UTC

**34.其他**

**设置登录前提示语**

root@SRX550# set system login message "Warning, Unauthorized access are forbidden!"

**设置console线拨出时自动退出console会话**

root@SRX550# set system ports console log-out-on-disconnect

**35.配置命令层次**

|  |  |  |
| --- | --- | --- |
| 第一层： | 第二层 | 说明 |
| system | host-name | 设置主机名 |
| time-zone | 设置时区 |
| root-authentication | 设置root密码 |
| name-server | 设置dns |
| login | 设置登录用户 |
| services | 设置登录服务 |
| syslog | 日志 |
| max-configurations-on-flash | 最大回滚数 |
| max-configuration-rollbacks | 最大回滚数 |
| processes |  |
| ntp | NTP |
| interfaces |  | 设置接口的ip |
| snmp |  |  |
| routing-options | static | 路由条目 |
| routing-instances |  | 路由实例，可用于策略路由 |
| policy-options | prefix-list | 防火墙过滤时的匹配前缀 |
| security | ike | proposal,policy,gateway |
| ipsec |  |
| utm |  |
| dynamic-vpn |  |
| flow |  |
| screen |  |
| nat |  |
| policies | 安全域之间的放行策略 |
| zones | 安全域的接口和地址簿 |
| firewall | family inet | 可filter过滤前缀地址 |
| filter | 可做策略路由 |
| access | profile | 可定义登录dvpn的用户 |
| address-assignment | 可定义分配给dvpn的地址 |
| firewall-authentication |  |
| applications | application | 定义端口号 |
| application-set | 定义端口组 |

**★原始配置**

root> show configuration

## Last commit: 2022-07-22 11:55:14 UTC by root

version 12.1X46-D35.1;

system {

autoinstallation {

delete-upon-commit; ## Deletes [system autoinstallation] upon change/commit

traceoptions {

level verbose;

flag {

all;

}

}

interfaces {

ge-0/0/0 {

bootp;

}

}

}

root-authentication {

encrypted-password "$1$rcM1lNXe$sc96V68EFlwalM1LQl3dt."; ## SECRET-DATA

}

name-server {

208.67.222.222;

208.67.220.220;

}

services {

ssh;

telnet;

xnm-clear-text;

web-management {

http {

interface vlan.0;

}

https {

system-generated-certificate;

interface vlan.0;

}

}

dhcp {

router {

192.168.1.1;

}

pool 192.168.1.0/24 {

address-range low 192.168.1.2 high 192.168.1.254;

}

propagate-settings ge-0/0/0.0;

}

}

syslog {

archive size 100k files 3;

user \* {

any emergency;

}

file messages {

any critical;

authorization info;

}

file interactive-commands {

interactive-commands error;

}

}

max-configurations-on-flash 5;

max-configuration-rollbacks 5;

license {

autoupdate {

url https:#ae1.juniper.net/junos/key\_retrieval;

}

}

}

interfaces {

ge-0/0/0 {

unit 0;

}

ge-0/0/1 {

unit 0 {

family ethernet-switching {

vlan {

members vlan-trust;

}

}

}

}

ge-0/0/2 {

unit 0 {

family ethernet-switching {

vlan {

members vlan-trust;

}

}

}

}

ge-0/0/3 {

unit 0 {

family ethernet-switching {

vlan {

members vlan-trust;

}

}

}

}

ge-0/0/4 {

unit 0 {

family ethernet-switching {

vlan {

members vlan-trust;

}

}

}

}

ge-0/0/5 {

unit 0 {

family ethernet-switching {

vlan {

members vlan-trust;

}

}

}

}

vlan {

unit 0 {

family inet {

address 192.168.1.1/24;

}

}

}

}

protocols {

stp;

}

security {

screen {

ids-option untrust-screen {

icmp {

ping-death;

}

ip {

source-route-option;

tear-drop;

}

tcp {

syn-flood {

alarm-threshold 1024;

attack-threshold 200;

source-threshold 1024;

destination-threshold 2048;

timeout 20;

}

land;

}

}

}

nat {

source {

rule-set trust-to-untrust {

from zone trust;

to zone untrust;

rule source-nat-rule {

match {

source-address 0.0.0.0/0;

}

then {

source-nat {

interface;

}

}

}

}

}

}

policies {

from-zone trust to-zone untrust {

policy trust-to-untrust {

match {

source-address any;

destination-address any;

application any;

}

then {

permit;

}

}

}

}

zones {

security-zone trust {

host-inbound-traffic {

system-services {

all;

}

protocols {

all;

}

}

interfaces {

vlan.0;

}

}

security-zone untrust {

screen untrust-screen;

interfaces {

ge-0/0/0.0 {

host-inbound-traffic {

system-services {

dhcp;

tftp;

}

}

}

}

}

}

}

vlans {

vlan-trust {

vlan-id 3;

l3-interface vlan.0;

}

}