Juniper SRX 防火墙配置教程

前言：

作者有幸接触到 Juniper SRX 系列的防火墙，但没有接受过 Juniper 的培训，也不知道在哪里有培训，只好自己在网上查找相关配置资料，不过想找一份比较全面的资料实在是太难了。大概查了一个多月的资料吧，现在也算是稍微弄懂了一点儿 SRX 系列的防火墙的配置。为了方便初学者的学习，故作此手册；如有不当之处，还请指正。

作者：李茂福　2019 年 9 月 24 日

说明：

（1）蓝色的字为配置命令，绿色的字为对命令的解析，有些地方命令比较密集的就不用蓝色标出了

（2）输入命令时要先弄清楚该命令是在哪个模式下输入的，看命令前的 shell 提示符

目录：

无目录，本文档发布时为 pdf 格式，可以查看书签，点击书签跳到相应的页面。

0. 搭建实验环境

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，我目前也没有注册成功过。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，也可联系我，Email: sysyear@163.com

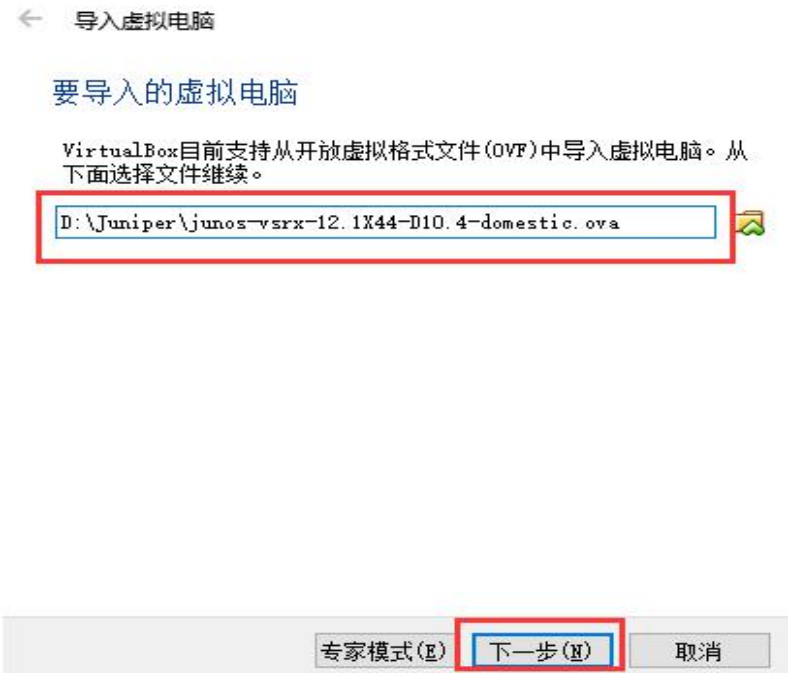
准备事项

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

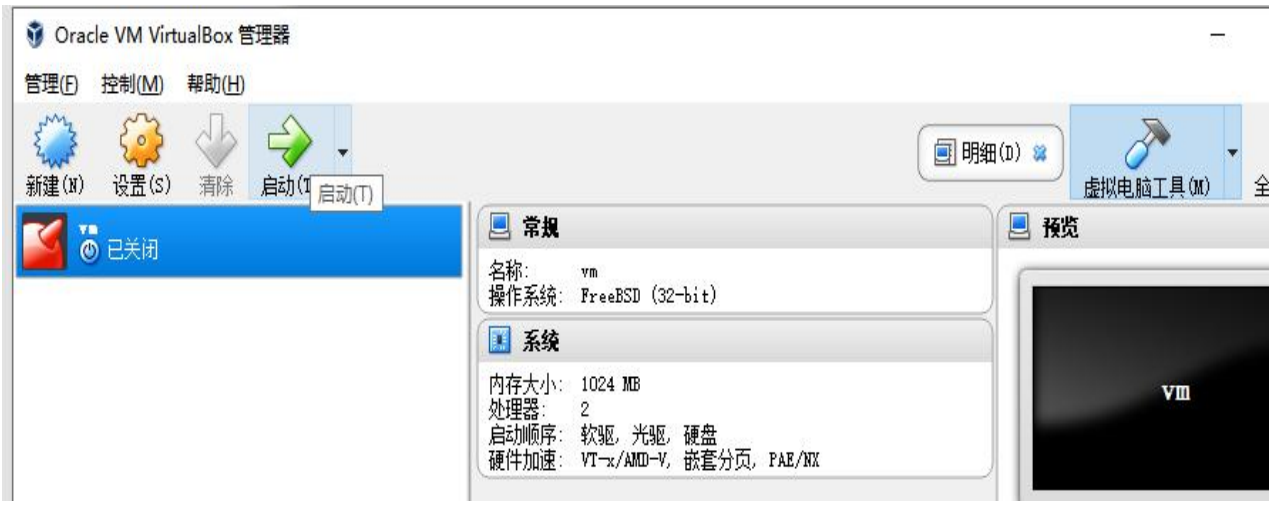
点击主界面左上角的“管理”，“导入虚拟电脑”

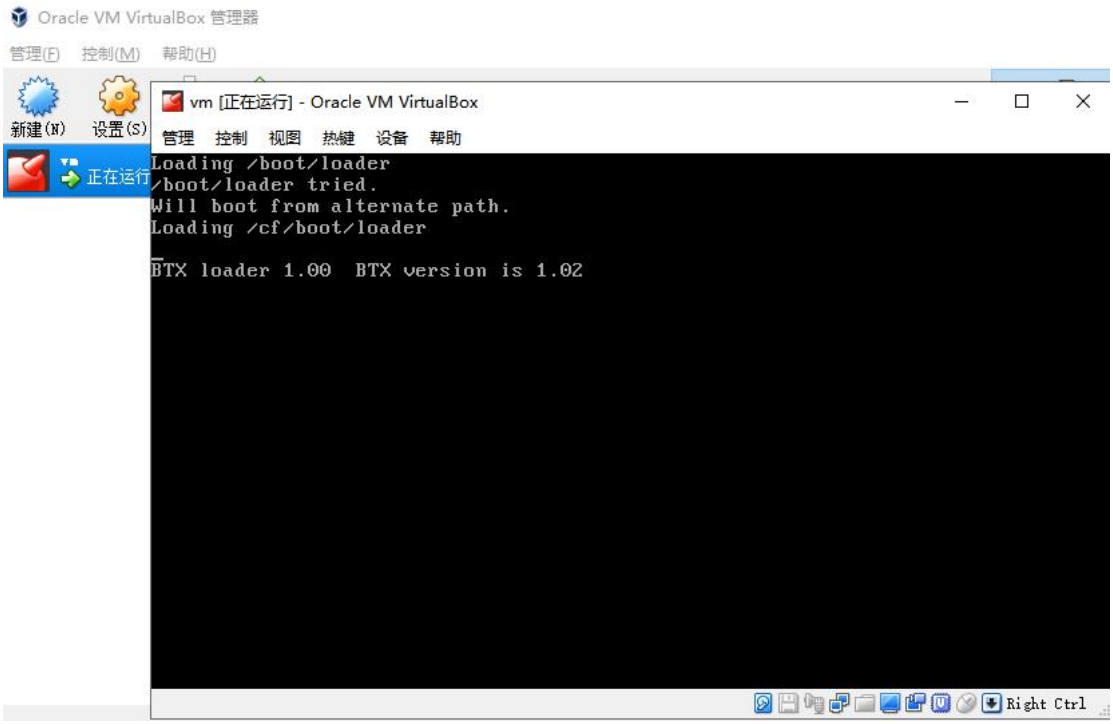
在“导入虚拟电脑”对话框中，选择之前下载的.ova 文件，如下图：



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



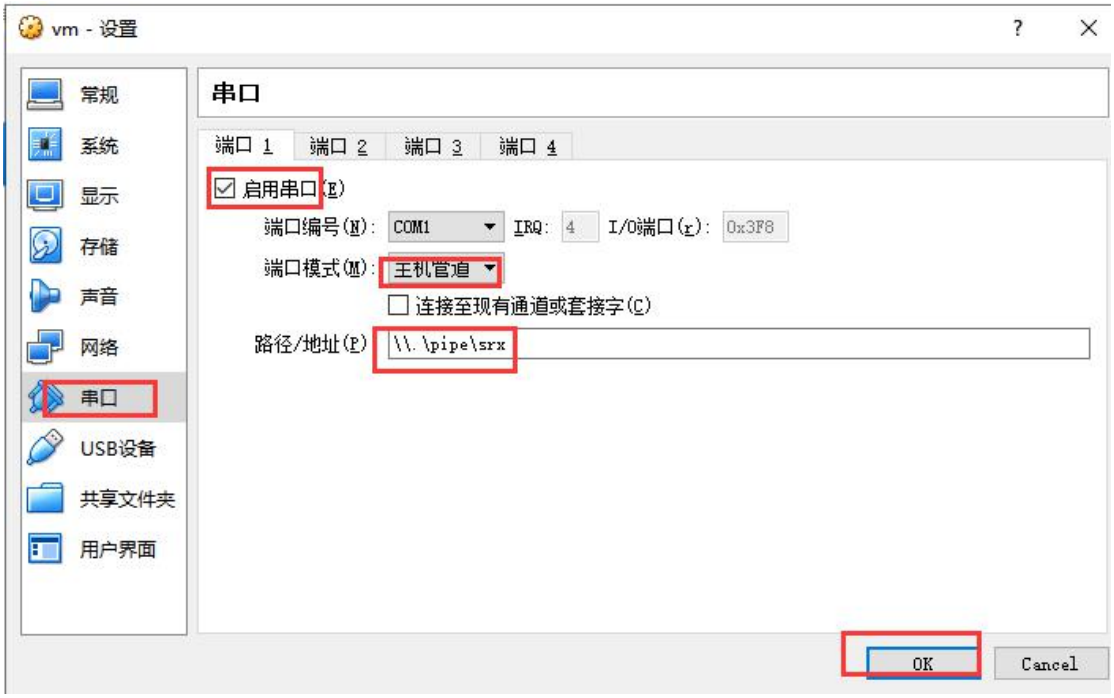


出现上图的界面就说明系统正在启动，需要的时间比较长，大概等待几分钟，，，，

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

1.初次登录（console 登录）

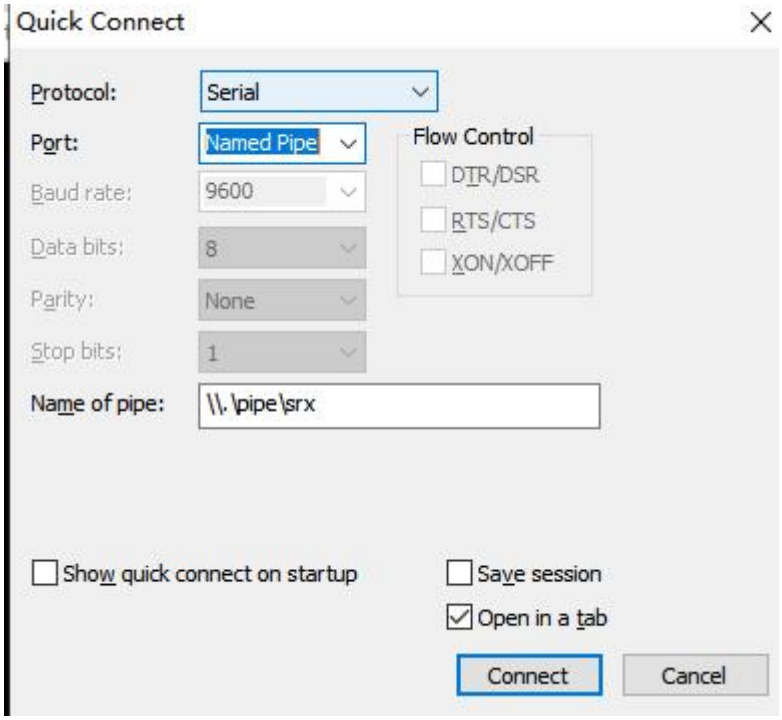
以 root 用户登录，初始密码为空，进入系统 cli 后，再进入配置模式，设置 root 密码


```
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
New password:
Retype new password:
```

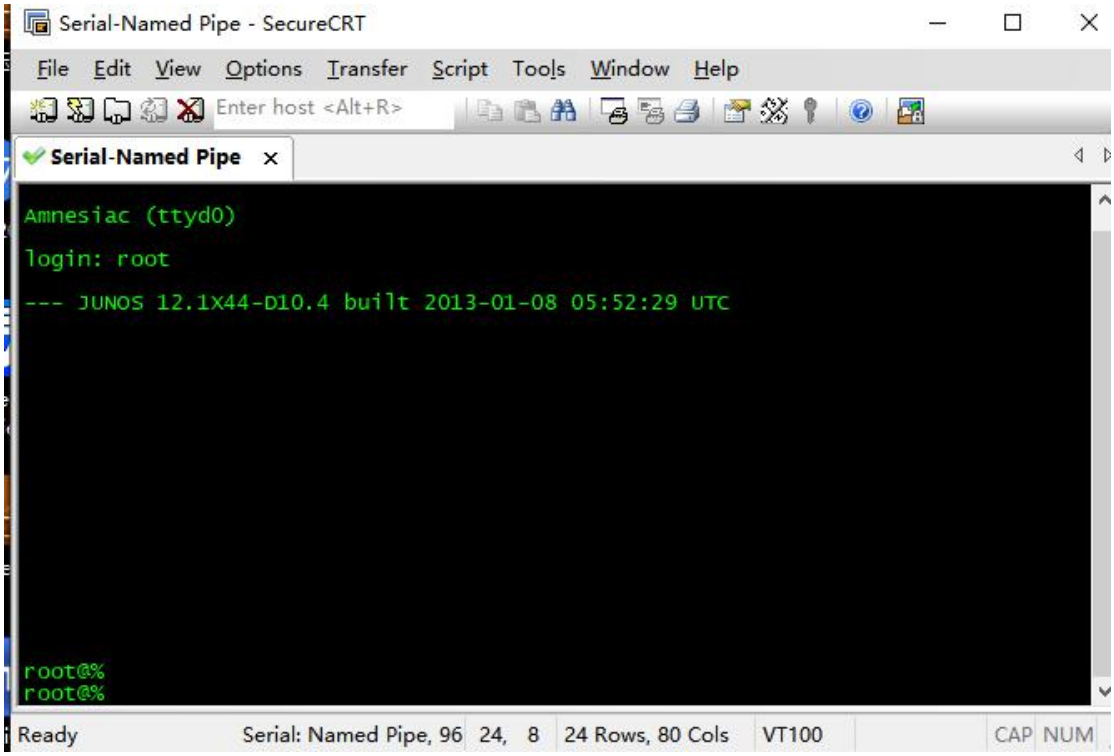
```
root# commit
commit complete

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#
```

2. 使用 SecureCRT 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



3.设置系统基本信息（主机名，时区，时间，DNS）

```
root# set system host-name SRX550   //主机名

[edit]
root@SRX550#
root@SRX550# set system time-zone Asia/Shanghai   //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，可以设置多条


root@SRX550# commit
commit complete

[edit]
root@SRX550# commit       //记得要两次提交
commit complete
```

4.创建用户

```
root@SRX550# set system login user coflee class super-user authentication
            plain-text-password
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
```

5.设置 console 输出的宽度和行数

```
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
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
```

6.接口加入安全域

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

[edit]

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

[edit]
```

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: On
  Policy configurable: Yes
  Interfaces bound: 1
  Interfaces:
    ge-0/0/0.0

Security zone: untrust
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
```

```
  Screen: untrust-screen
  Interfaces bound: 1
  Interfaces:
    ge-0/0/1.0

Security zone: junos-host
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: 0
  Interfaces:
```

7.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

[edit]
```

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
dsc                     up    up
```

8.配置缺省/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
```

9.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
```

10.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)
[edit]
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

11.放行服务

```
root@SRX550#  set  security  zones  security-zone  trust  host-inbound-traffic
system-services all    //或具体的服务，如下：
root@SRX550#  set  security  zones  security-zone  untrust  host-inbound-traffic
system-services ping
root@SRX550#  set  security  zones  security-zone  untrust  host-inbound-traffic
system-services telnet
root@SRX550#  set  security  zones  security-zone  untrust  host-inbound-traffic
system-services ssh
root@SRX550#  set  security  zones  security-zone  untrust  host-inbound-traffic
system-services https
```

12.放行安全域之间的流量 策略

```
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

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;
                }
            }
        }
policies {  //系统默认
        from-zone trust to-zone trust {
            policy default-permit {
                match {
                    source-address any;
                    destination-address any;
                    application any;
                }
                then {
                    permit;
                }
            }
        }
        from-zone trust to-zone untrust {  //系统默认
            policy default-permit {
                match {
                    source-address any;
                    destination-address any;
                    application any;
                }
                then {
                    permit;
                }
            }
        }
```

13.删除默认的 deny 策略

```
root@SRX550# delete security policies from-zone untrust to-zone trust policy
             default-deny
```

```
security polices  from-zone untrust to-zone trust {
             policy default-deny {
                 match {
                     source-address any;
                     destination-address any;
                     application any;
                 }
                 then {
                     deny;
                 }
             }
```

再添加其他的 deny，放到最后

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
```

当一个接口上有多个 IP 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
```

15.目的 NAT ，端口映射

```
root@SRX550# set security nat destination pool towebser address 192.168.1.10 port
             80
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
root@SRX550# set security nat destination rule-set r_towebser rule r1 match
             destination-port 2333
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_2333 protocol tcp destination-port
             2333
root@SRX550# set security zones security-zone trust address-book address
             ab_192.168.1.10 192.168.1.10/32
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_2333
root@SRX550# set security policies from-zone untrust to-zone trust policy
             p_towebser then permit
```

16.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

[edit]
root@SRX550#


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]
```

17.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

18.基本维护查看命令

```
root@SRX550> show system users
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
Information for junos:
Comment:
JUNOS Software Release [12.1X44-D10.4]


root@SRX550> show system uptime
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                                49d35a19e417      JUNOSV-FIREFLY
Midplane
System IO
Routing Engine                                            JUNOSV-FIREFLY RE
FPC 0                                                     Virtual FPC
  PIC 0                                                   Virtual GE
Power Supply 0

root@SRX550> show chassis firmware
Part                    Type       Version
FPC                     O/S        Version 12.1X44-D10.4 by builder on 2013-01
FWDD                    O/S        Version 12.1X44-D10.4 by builder on 2013-01

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
```

```
>show route
>show arp
>show interface terse
>show log
```

```
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.
```

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，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
```

25.查看配置

```
root@SRX550> show configuration     //查看已保存的配置
## Last commit: 2019-09-20 14:50:58 CST by root
version 12.1X44.4;
system {
```

```
    host-name SRX550;
    ... ...

root@SRX550# show
## Last changed: 2019-09-20 14:50:58 CST
version 12.1X44.4;
system {
    host-name SRX550;
    ... ...

root@SRX550# run show configuration          //查看正在运行的配置
## Last commit: 2019-09-20 14:50:58 CST by root
version 12.1X44.4;
system {
    host-name SRX550;
    ... ...
```

26.保存系统配置、以配置文件恢复

```
root@SRX550# save conf.cfg    //保存的文件名为 conf.cfg，可以随便命名
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

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
```

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
```

27.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
```

28.设备停机、重启

```
root@Test-SRX> request system halt       //重启为 request system reboot
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
```

29.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
```

30.boot 模式下升级系统

重启或开机时出现如下行时按下空格

```
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 ?            //输入问号可以查看支持的命令
Available commands:
  reboot            reboot the system
  heap              show heap usage
  bcachestat        get disk block cache stats
  boot              boot a file or loaded kernel
  autoboot          boot automatically after a delay
  help              detailed help
  ?                 list commands
  show              show variable(s)
  set               set a variable
  unset             unset a variable
  echo              echo arguments
  read              read input from the terminal
  more              show contents of a file
  nextboot          set next boot device
  install           install JUNOS
  include           read commands from a file
  ls                list files
  load              load a kernel or module
  unload            unload all modules
  lsmod             list loaded modules
  pnpscan           scan for PnP devices
  recover           initiate recovery process from compact flash
  boot-conf         load kernel and modules, then autoboot
  read-conf         read a configuration file
  enable-module     enable loading of a module
  disable-module    disable loading of a module
  toggle-module     toggle loading of a module
  show-module       show module load data

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
```

31.恢复密码，原配置不变（进入 boot 模式）

```
OK boot -s     //进入单用户模式
.......
Enter full pathname of shell or 'recovery' for root password recovery or RETURN for
/bin/sh: recovery
.......
Starting CLI ...
root@Test-SRX> configure
root@Test-SRX# delete system root-authentication
root@Test-SRX# set system root-authentication plain-text-password
New password:
Retype new password:

[edit]
root@Test-SRX# commit
commit complete

[edit]
root@Test-SRX# commit
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#
```

```
root@Test-SRX> request system reboot          //要重启系统，进入正常的模式
Reboot the system ? [yes,no] (no) yes

Shutdown NOW!
[pid 1374]
```

32.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
```

33.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

10000.系统启动过程：

```
Rebooting...
cpu_reset: Stopping other CPUs
Consoles: serial port
BIOS drive A: is disk0
BIOS drive C: is disk1
BIOS 639kB/1047488kB available memory

FreeBSD/i386 bootstrap loader, Revision 1.2
(builder@briath.juniper.net, Tue Jan  8 04:04:34 UTC 2013)
Loading /boot/defaults/loader.conf
/kernel text=0x894aa0 data=0x4d050+0x100b2c syms=[0x4+0x92cf0+0x4+0xd1487]
/boot/modules/libmbpool.ko text=0xd9c data=0x100
/boot/modules/if_em_vjx.ko text=0xb794 data=0x5ec+0x204 /



Hit [Enter] to boot immediately, or space bar for command prompt.
Booting [/kernel]...
platform_early_bootinit: Early Boot Initialization
GDB: debug ports: sio
GDB: current port: sio
KDB: debugger backends: ddb gdb
KDB: current backend: ddb
Copyright (c) 1996-2013, Juniper Networks, Inc.
All rights reserved.
Copyright (c) 1992-2006 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
        The Regents of the University of California. All rights reserved.
JUNOS 12.1X44-D10.4 #0: 2013-01-08 05:52:29 UTC

builder@briath.juniper.net:/volume/build/junos/12.1/service/12.1X44-D10.4/obj-i
386/junos/bsd/kernels/VSRX/kernel
Timecounter "i8254" frequency 1193182 Hz quality 0
CPU: Intel(R) Core(TM) i5-8400 CPU @ 2.80GHz (2808.01-MHz 686-class CPU)
  Origin = "GenuineIntel"  Id = 0x906ea  Stepping = 10

Features=0x1783fbff<FPU,VME,DE,PSE,TSC,MSR,PAE,MCE,CX8,APIC,SEP,MTRR,PGE,MCA,CM
OV,PAT,PSE36,MMX,FXSR,SSE,SSE2,HTT>

Features2=0x56da2203<SSE3,<b1>,SSSE3,CX16,<b17>,SSE4.1,SSE4.2,MOVBE,POPCNT,<b25
>,XSAVE,<b28>,<b30>>
  AMD Features=0x8100000<NX,RDTSCP>
  AMD Features2=0x121<LAHF,ABM,Prefetch>
```

```
  Cores per package: 2
real memory  = 1073676288 (1023 MB)
avail memory = 587489280 (560 MB)
MPTable: <VBOXCPU  VirtualBox  >
FreeBSD/SMP: Multiprocessor System Detected: 2 CPUs
 cpu0 (BSP): APIC ID:  0
 cpu1 (AP): APIC ID:  1
pnpbios: Bad PnP BIOS data checksum
ioapic0: Assuming intbase of 0
ioapic0 <Version 2.0> irqs 0-23 on motherboard
netisr_init: !debug_mpsafenet, forcing maxthreads from 2 to 1
Initializing VSRX platform properties ..
cpu0 on motherboard
cpu1 on motherboard
pcib0: <Host to PCI bridge> pcibus 0 on motherboard
pir0: <PCI Interrupt Routing Table: 30 Entries> on motherboard
pci0: <PCI bus> on pcib0
isab0: <PCI-ISA bridge> at device 1.0 on pci0
isa0: <ISA bus> on isab0
atapci0:        <Intel        PIIX4        UDMA33        controller>        port
0x1f0-0x1f7,0x3f6,0x170-0x177,0x376,0xd000-0xd00f at device 1.1 on pci0
ata0: <ATA channel 0> on atapci0
ata1: <ATA channel 1> on atapci0
pci0: <display, VGA> at device 2.0 (no driver attached)
pci0: <base peripheral> at device 4.0 (no driver attached)
pci0: <multimedia, audio> at device 5.0 (no driver attached)
piix0: PIIX I/O space not mapped
smb0: <Intel 82371AB SMB controller> irq 9 at device 7.0 on pci0
em0: <Intel(R) PRO/1000 Network Connection - VJX stub Version - 3.2.18> port
0xd240-0xd247 mem 0xf0420000-0xf043ffff irq 11 at device 8.0 on pci0
em1: <Intel(R) PRO/1000 Network Connection - VJX stub Version - 3.2.18> port
0xd248-0xd24f mem 0xf0440000-0xf045ffff irq 11 at device 17.0 on pci0
orm0: <ISA Option ROM> at iomem 0xc0000-0xc7fff on isa0
atkbdc0: <Keyboard controller (i8042)> at port 0x60,0x64 on isa0
atkbd0: <AT Keyboard> irq 1 on atkbdc0
kbd0 at atkbd0
psm0: <PS/2 Mouse> irq 12 on atkbdc0
psm0: model IntelliMouse Explorer, device ID 4
vga0: <Generic ISA VGA> at port 0x3c0-0x3df iomem 0xa0000-0xbffff on isa0
sc0: <System console> at flags 0x100 on isa0
sc0: VGA <16 virtual consoles, flags=0x100>
sio0 at port 0x3f8-0x3ff irq 4 flags 0x90 on isa0
sio0: type 16550A, console
sio1: configured irq 5 not in bitmap of probed irqs 0
```

```
sio1: port may not be enabled
sio2: configured irq 3 not in bitmap of probed irqs 0
sio2: port may not be enabled
sio3: configured irq 7 not in bitmap of probed irqs 0
sio3: port may not be enabled
Initializing product: 131 ..
###PCB Group initialized for udppcbgroup
###PCB Group initialized for tcppcbgroup
ad0: Device does not support APM
ad0: 2048MB <VBOX HARDDISK 1.0> at ata0-master UDMA33
SMP: AP CPU #1 Launched!
Trying to mount root from ufs:/dev/ad0s1a
Attaching /cf/packages/junos via /dev/mdctl...
Mounted junos package on /dev/md0...

Automatic reboot in progress...
** /dev/ad0s1a
FILE SYSTEM CLEAN; SKIPPING CHECKS
clean, 710018 free (18 frags, 177500 blocks, 0.0% fragmentation)
** /dev/ad0s1e
FILE SYSTEM CLEAN; SKIPPING CHECKS
clean, 102774 free (2 frags, 25693 blocks, 0.0% fragmentation)
Verified junos signed by PackageProduction_12_1_0
Verified jboot signed by PackageProduction_12_1_0
Verified junos-vsrx-12.1X44-D10.4-domestic signed by PackageProduction_12_1_0
Loading configuration ...
mgd: commit complete
Setting initial options: .
Starting optional daemons: .
Doing initial network setup:.
Initial interface configuration:
additional daemons: eventd.
Additional routing options:kern.module_path: /boot//kernel;/boot/modules ->
/boot/modules;/modules/peertype;/modules/ifpfe_drv;/modules/ifpfe_media;/module
s/platform;/modules;
kld netpfe media: ifpfem_bri ifpfem_ds0 ifpfem_ds1e1 ifpfem_ds3e3kld netpfe drv:
ifpfed_atm ifpfed_controller ifpfed_dialer ifpfed_ds0 ifpfed_ds1e1 ifpfed_ds3e3
ifpfed_eia530 ifpfed_eth ifpfed_irb ifpfed_isdn ifpfed_ism ifpfed_lt
ifpfed_ml_cmnK ifpfed_ml_haL ifpfed_modemD ifpfed_modem.ko: depends on ucom - not
available
kldload: can't load /modules/ifpfe_drv/ifpfed_modem.ko: No such file or directory
 ifpfed_ppeer ifpfed_pppoe ifpfed_st ifpfed_svcs ifpfed_vp ifpfed_vtkld platform:
fileassoc if_em_vjx ifpfem_xdsl ixp j_ifpfekld peertype: peertype_fwdd
peertype_pfpc peertype_slavere ipsec kld resrsv.
```

```
Doing additional network setup:.
Starting final network daemons:.
setting ldconfig path: /usr/lib /opt/lib
ldconfig: warning: /opt/lib: No such file or directory
starting standard daemons: cron.
Initial rc.i386 initialization:.

 Lock Manager
RDM Embedded 7 [04-Aug-2006] http://www.birdstep.com
Copyright (c) 1992-2006 Birdstep Technology, Inc.  All Rights Reserved.

Unix Domain sockets Lock manager
Lock manager 'lockmgr' started successfully.
Error: Profile database dictionary file missing.
Profile database initialized
Local package initialization:.
starting local daemons:.
kern.securelevel: -1 -> 1
The inital provisioning tool works for VMware only.
Fri Sep 20 15:28:23 CST 2019

Test-SRX (ttyd0)

login:
```