



vSRX2.0 Junos 15.1-x49-d15.4 on VMware Fusion on MacOSX

Purpose: setup a vSRX2.0 image under VMware Fusion on a MacOSX

Author: Laurent Paumelle – Juniper Center of Excellence

Date: August, 24th 2015

Versions:

VMware Fusion version 7.1.2

vSRX 2.0 version Junos 15.1-x49-d15.4

Release Note:

http://www.juniper.net/techpubs/en_US/vsrx15.1x49/information-products/topic-collections/release-notes/15.1x49/vsrx-release-notes.pdf

Virtual version vSRX:

<http://www.juniper.net/support/downloads/?p=vsrx#sw>

for VMware IDE drive version:

<https://webdownload.juniper.net/swdl/dl/secure/site/1/record/59596.html>

Overall procedure:

- import OVA
- use/create a Management network with your Mac (Host-only is ok)
- use/create a Left/Trust network for the other hosts behind the vSRX: do not use DHCP offer from VMware, vSRX will do it
- use/create a Right/Untrust network for the external interface of the vSRX, used to access internet (sharing the existing Bridge or Shared NAT is ok)
- customize the memory and cpu settings
- run the vSRX and customize it using the console
- set the minimal admin and network settings
- access using ssh and complete the configuration
- wait for all interfaces to come up
- create a client VM behind it and access internet



Step by step procedure:

Import the OVA:

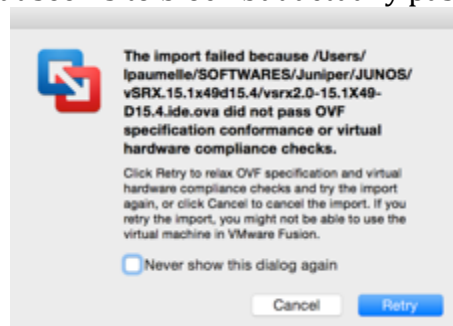


and specify the target new VM destination image.

Accept the license agreement:



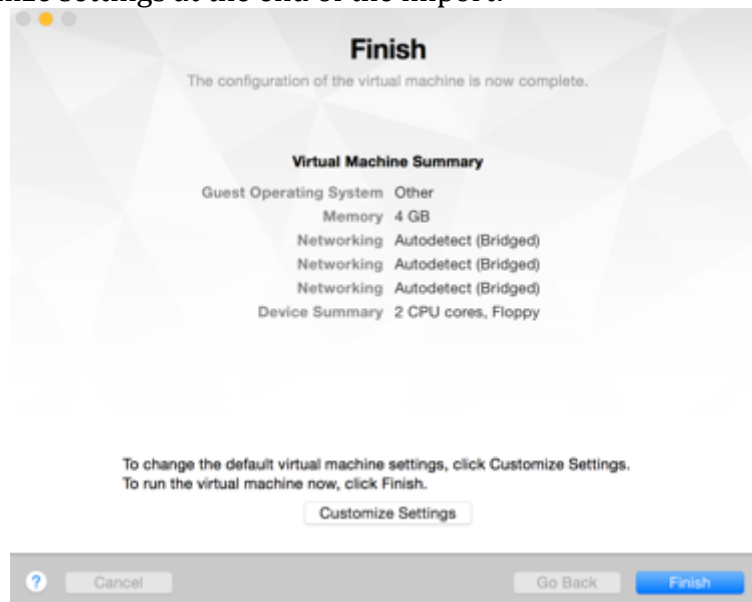
Retry the OVA check that seems to block but actually pass:



Importation in progress:



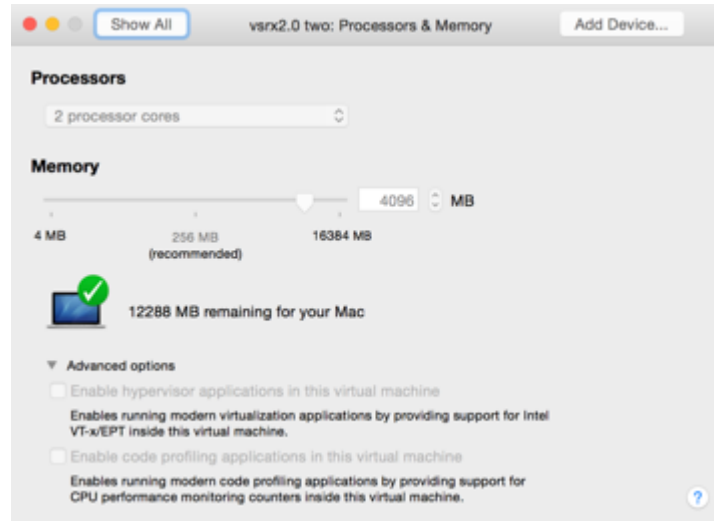
Then customize settings at the end of the import:



Processors and Memory:

Minimum required ([release notes](#)):

- 2 cores
- 4G RAM



Not specified is the “Enable hypervisor”. But it does work also without, though the Junos itself is also a VM inside the base linux OS.
Tested on an other vSRX VM with the VT-x turned on also worked normally.

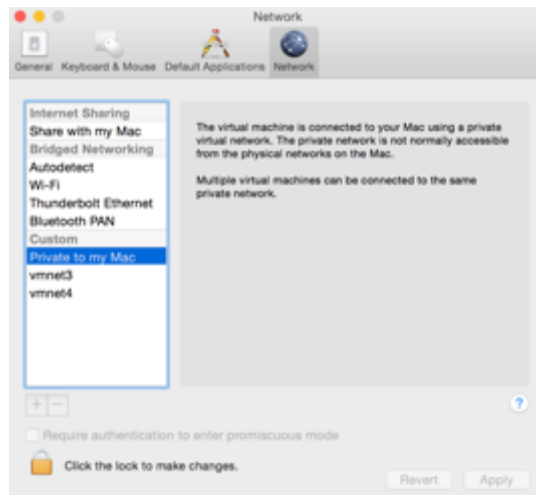
**1st Network Adapter : fxp0 (management)**

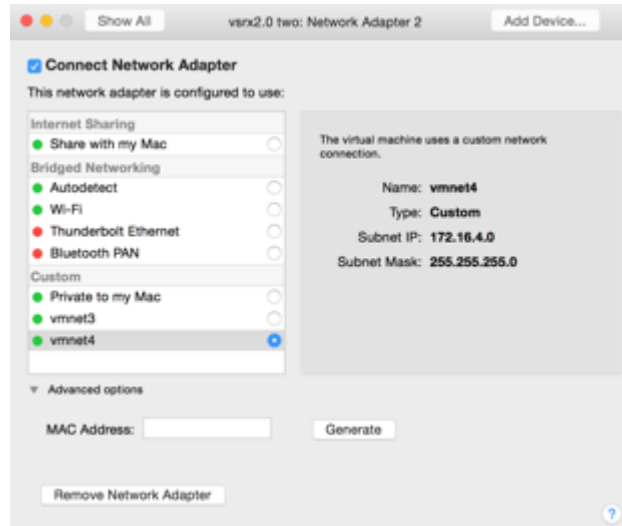
it can be set to communicate with the Mac only so “Private to my Mac” is a perfect use.



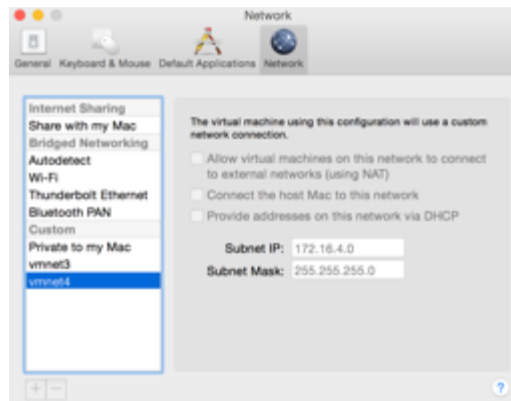
Settings for that network (Vmware Fusion preferences menu):

Require authentication to enter for Promiscuous mode was set to false as it is needed for the fxp0.

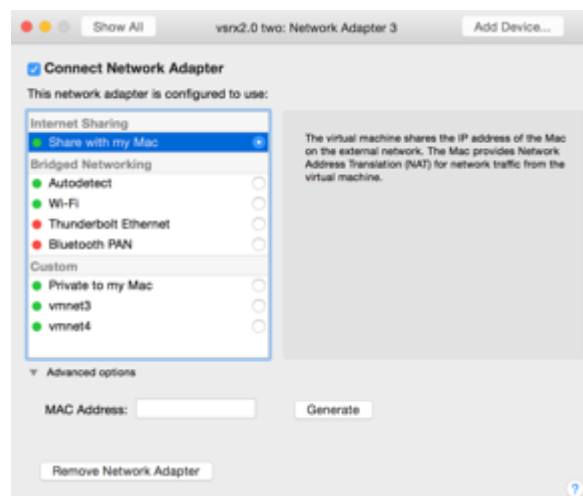
**2nd Network Adapter : ge-0/0/0 (trust)**



Settings for that network (Vmware Fusion preferences menu):
new vmnet4 not shared with the Mac but with other VMs as client/protected by the vSRX.

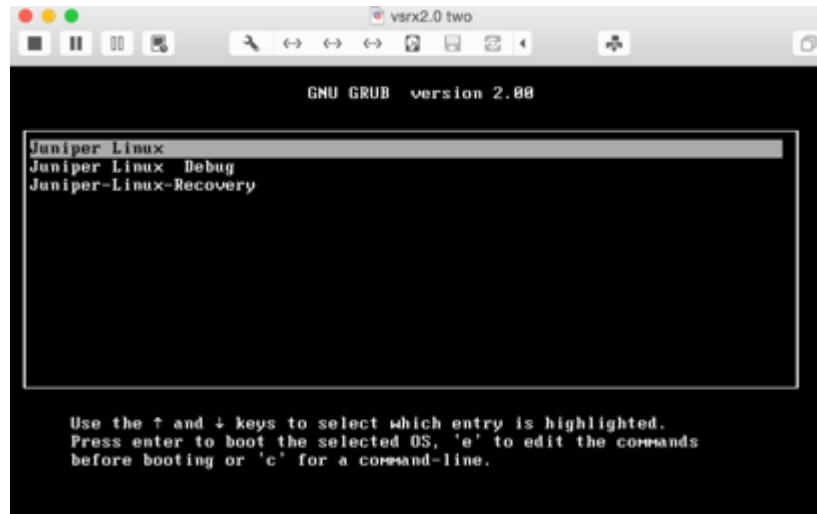


3rd Network Adapter : ge-0/0/1 (untrust)





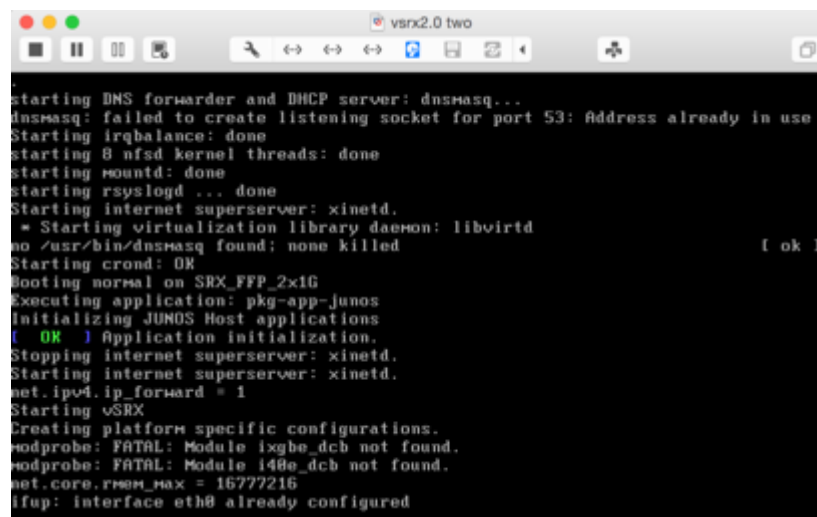
Booting vSRX2.0:



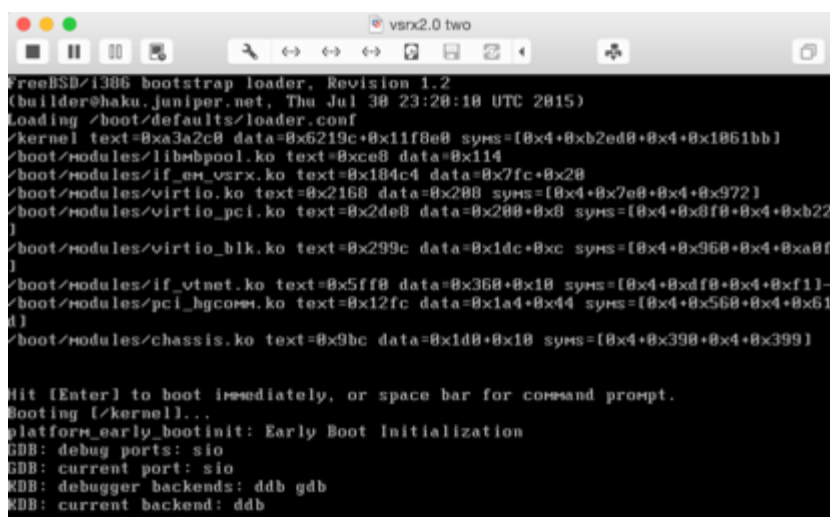
```
GNU GRUB version 2.00

Juniper Linux
Juniper Linux Debug
Juniper-Linux-Recovery

Use the ↑ and ↓ keys to select which entry is highlighted.
Press enter to boot the selected OS, 'e' to edit the commands
before booting or 'c' for a command-line.
```



```
starting DNS forwarder and DHCP server: dnsmasq...
dnsmasq: failed to create listening socket for port 53: Address already in use
Starting irqbalance: done
Starting 8 nfsd kernel threads: done
Starting mountd: done
Starting rsyslogd ... done
Starting internet superserver: xinetd.
* Starting virtualization library daemon: libvirt
no /usr/bin/dnsmasq found: none killed [ ok ]
Starting crond: OK
Booting normal on SRX_FFP_2x1G
Executing application: pkg-app-junos
Initializing JUNOS Host applications
[ OK ] Application initialization.
Stopping internet superserver: xinetd.
Starting internet superserver: xinetd.
net.ipv4.ip_forward = 1
Starting vSRX
Creating platform specific configurations.
modprobe: FATAL: Module ixgbe_dcb not found.
modprobe: FATAL: Module i40e_dcb not found.
net.core.rmem_max = 16777216
ifup: interface eth0 already configured
```



```
FreeBSD/1306 bootstrap loader, Revision 1.2
(builder@haku.juniper.net, Thu Jul 30 23:20:10 UTC 2015)
Loading /boot/defaults/loader.conf
/kernel text=0xa3a2c0 data=0x6218c+0x11f8e0 syms=[0x4+0xb2ed0+0x4+0x1061bb]
/boot/modules/libmbpool.ko text=0xc0e8 data=0x114
/boot/modules/if_em_vsr.ko text=0x104c4 data=0x7fc+0x28
/boot/modules/virtio.ko text=0x2160 data=0x200 syms=[0x4+0x7e0+0x4+0x972]
/boot/modules/virtio_pci.ko text=0x2de0 data=0x200+0x8 syms=[0x4+0x8f8+0x4+0xb22]
/boot/modules/virtio_blk.ko text=0x299c data=0x1dc+0xc syms=[0x4+0x960+0x4+0xa8f]
/boot/modules/if_vnet.ko text=0x5ff0 data=0x360+0x10 syms=[0x4+0xdf8+0x4+0xf11]
/boot/modules/pci_hgcom.ko text=0x12fc data=0x1a4+0x44 syms=[0x4+0x560+0x4+0x61]
/boot/modules/chassis.ko text=0x9bc data=0x1d0+0x10 syms=[0x4+0x390+0x4+0x399]

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
GDB: debugger backends: ddb gdb
GDB: current backend: ddb
```

some minutes later, after generating RSA private and public keys and launching services, it gets to the console login:



```
vsrx2.0 two
setting ldconfig path: /usr/lib /opt/lib
ldconfig: /opt/lib: ignoring directory not owned by root
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:set cores for group access
.
kern.securelevel: -1 -> 1
The machine id is empty.
Cleaning up ...
Mon Aug 24 13:26:34 UTC 2015
Aug 24 13:26:35 init: exec_command: /usr/sbin/dhcpd (PID 1421) started
Amnesiac (ttyd8)
login: _
```

Enter the root (no password for first run) and cli as of anu standard first boot Junos:

```
vsrx2.0 two
Error: Profile database dictionary file missing.
Profile database initialized
Local package initialization:.
starting local daemons:set cores for group access
.
kern.securelevel: -1 -> 1
The machine id is empty.
Cleaning up ...
Mon Aug 24 13:26:34 UTC 2015
Aug 24 13:26:35 init: exec_command: /usr/sbin/dhcpd (PID 1421) started
Amnesiac (ttyd8)
login: root
--- JUNOS 15.1X49-D15.4 built 2015-07-31 02:20:21 UTC
root%
root% cli
root>
root> edit
Entering configuration mode
[edit]
root# _
```

and set all necessary parameters such as the below for example:

```
root# set system root-authentication plain-text-password
New password:
Retype new password:
```

And some basic configuration (network, zones):

```
set system name-server 8.8.8.8

set security zones security-zone trust interfaces ge-0/0/0.0 host-inbound-traffic system-services all

set security zones security-zone untrust interfaces ge-0/0/1.0 host-inbound-traffic system-services dhcp
set security zones security-zone untrust interfaces ge-0/0/1.0 host-inbound-traffic system-services ping

set interfaces ge-0/0/0 unit 0 family inet address 192.168.0.1/24
set interfaces ge-0/0/1 unit 0 family inet dhcp
set interfaces fxp0 unit 0 family inet dhcp

commit check
commit and-quit
```




Admin connection via fxp0:

Via the command line tools under MacOSx (terminal or iterm):

```

bash
bash-3.2$ ssh root@192.168.70.130
The authenticity of host '192.168.70.130 (192.168.70.130)' can't be established.
RSA key fingerprint is de:cb:73:6c:e5:62:00:b3:0b:88:f7:24:ac:54:08:55.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.70.130' (RSA) to the list of known hosts.
Password:
--- JUNOS 15.1X49-D15.4 built 2015-07-31 02:20:21 UTC
mB6djbociUvOck3p6ehlAsZ04VxLeOnhnynC0yz300rlw62uJstXPVEsx00/UQE2d

```

ssh to the device :

Check connectivity to internet and name resolution, time, etc:

```

root> show interfaces terse | match inet
ge-0/0/0.0          up    up    inet    192.168.130.1/24
sp-0/0/0.0          up    up    inet
                    inet6
sp-0/0/0.16383      up    up    inet
ge-0/0/1.0          up    up    inet    172.16.30.140/24
em0.0               up    up    inet    128.0.0.1/2
em1.32768           up    up    inet    192.168.1.2/24
fxp0.0              up    up    inet    192.168.70.130/24
lo0.16384            up    up    inet    127.0.0.1      --> 0/0
lo0.16385            up    up    inet    10.0.0.1       --> 0/0

root> show route

inet.0: 7 destinations, 7 routes (7 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

0.0.0.0/0           *[Access-internal/12] 00:02:57
                    > to 172.16.30.2 via ge-0/0/1.0
172.16.30.0/24      *[Direct/0] 00:02:57
                    > via ge-0/0/1.0
172.16.30.140/32    *[Local/0] 00:02:57
                    Local via ge-0/0/1.0
192.168.70.0/24     *[Direct/0] 00:02:57
                    > via fxp0.0
192.168.70.130/32   *[Local/0] 00:02:57
                    Local via fxp0.0
192.168.130.0/24    *[Direct/0] 00:03:06
                    > via ge-0/0/0.0
192.168.130.1/32    *[Local/0] 00:03:06
                    Local via ge-0/0/0.0

root> ping www.cnn.con
^C
root> ping www.cnn.com
ping: cannot resolve www.cnn.com: Host name lookup failure

root> ping 4.2.2.3
PING 4.2.2.3 (4.2.2.3): 56 data bytes
64 bytes from 4.2.2.3: icmp_seq=0 ttl=128 time=53.133 ms
^C
--- 4.2.2.3 ping statistics ---
2 packets transmitted, 1 packets received, 50% packet loss
round-trip min/avg/max/stddev = 53.133/53.133/53.133/0.000 ms

root> show system license
License usage:

Feature name          Licenses    Licenses    Licenses    Expiry
                      used        installed   needed
Virtual Appliance     1           1           0           59 days

Licenses installed:
License identifier: E420588955
License version: 4
Software Serial Number: 20150625
Customer ID: vSRX-JuniperEval
Features:

```



And copy/paste whatever is missing (DNS, Time, NAT, DHCP services...).

Sample config:

```
set system time-zone Europe/Paris
set system name-server 8.8.8.8
set system name-server 4.2.2.2
set system name-server 4.2.2.1
set system login user laurent uid 2000
set system login user laurent class super-user
set system login user laurent authentication encrypted-password
"$1$4kJP6e24$wEeSC7QbHoI62pRFK7CUV."
set system login user laurent authentication ssh-rsa "ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQDe8Hr1x+zwnPYQda58287fJr4jCnoAYqVS0viK5rezqg8K4B
qKb5cRxTHV3HKKykCneRqRYz+jxncXbV6R3tdfYIoAYaZAbiH5GZqL+8f/xljhdxtQ2ncIyJiubpID
ekWioJkPp+WlJkoplSktGyVfpgGmt8DSEXZcRB4UKPwbPLjcQ8qk5ewuur161l+w414SvFCJbPlIep
bg4XXcRjsnNAIo36hLL/L09mB6dJbociUvOCK3p6ehlAsZ04VxLeOnhnynC0yz300rIw62uJsfXPVE
sx00/UQE2dz2Pvp4HUYCtiNbWPIqDMmi1fAER0XeVPfy2mkiPxjxlk8lDUBN
lpaumelle@juniper.net"

set system services dhcp name-server 4.2.2.1
set system services dhcp name-server 4.2.2.2
set system services dhcp domain-search juniper.net
set system services dhcp router 192.168.0.1
set system services dhcp pool 192.168.0.0/24 address-range low 192.168.0.100
set system services dhcp pool 192.168.0.0/24 address-range high 192.168.0.200

set system ntp server 81.170.151.60
set system ntp server 195.46.37.22

set security nat source rule-set Zone_trust-Zone_untrust from zone trust
set security nat source rule-set Zone_trust-Zone_untrust to zone untrust
set security nat source rule-set Zone_trust-Zone_untrust rule Group-
Nat2Internet match source-address 0.0.0.0/0
set security nat source rule-set Zone_trust-Zone_untrust rule Group-
Nat2Internet match destination-address 0.0.0.0/0
set security nat source rule-set Zone_trust-Zone_untrust rule Group-
Nat2Internet then source-nat interface

set security zones security-zone trust tcp-rst
set security zones security-zone trust interfaces ge-0/0/0.0 host-inbound-
traffic system-services all

set security zones security-zone untrust screen untrust-screen
set security zones security-zone untrust interfaces ge-0/0/1.0 host-inbound-
traffic system-services dhcp
set security zones security-zone untrust interfaces ge-0/0/1.0 host-inbound-
traffic system-services ping

set interfaces ge-0/0/0 unit 0 family inet address 192.168.0.1/24
set interfaces ge-0/0/1 unit 0 family inet dhcp
set interfaces fxp0 unit 0 family inet dhcp

commit check
commit and-quit
```

Wait a little bit before being able to go to internet for the interfaces to come up.

Create an other client VM and place it on the same vmnet4 network and try to access internet from it.