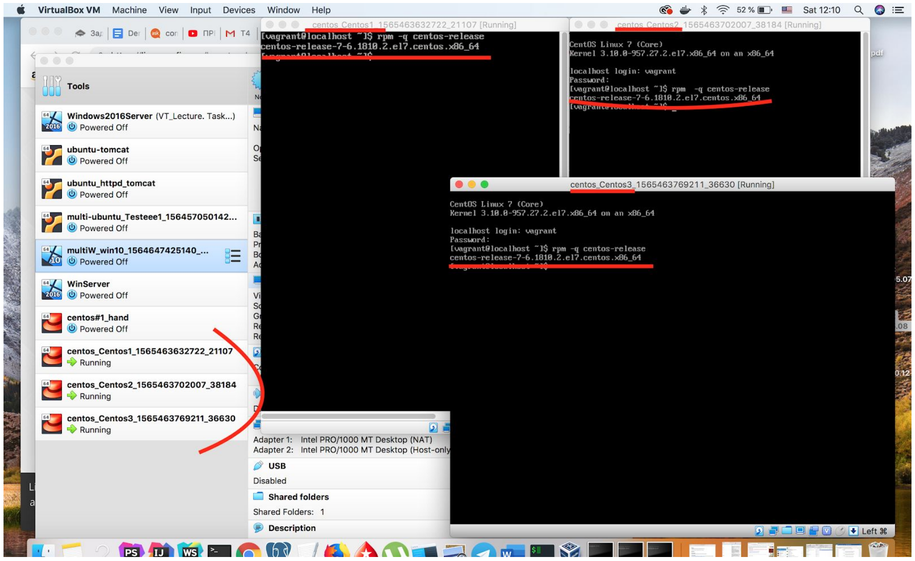
Dennis Tikhomirov **DevOps training, Spring’19 Homework**

Task 4. Networks, IPtables

1.Create 3 VMs with:

- **Centos 7 minimal**
- **Nat interface (must be disabled at the beginning)**
- **Host-only interface (must be disabled at the beginning)**



centos_Centos1_1565463632722_21107 [Running]

```
[vagrant@localhost ~]$ rpm -q centos-release
centos-release-7-6.1810.2.el7.centos.x86_64
[vagrant@localhost ~]$
```

centos_Centos2_1565463702007_38184 [Running]

```
CentOS Linux 7 (Core)
Kernel 3.10.0-957.27.2.el7.x86_64 on an x86_64

localhost login: vagrant
Password:
[vagrant@localhost ~]$ rpm  -q centos-release
centos-release-7-6.1810.2.el7.centos.x86_64
[vagrant@localhost ~]$ _
```

centos_Centos3_1565463769211_36630 [Running]

```
CentOS Linux 7 (Core)
Kernel 3.10.0-957.27.2.el7.x86_64 on an x86_64

localhost login: vagrant
Password:
[vagrant@localhost ~]$ rpm -q centos-release
centos-release-7-6.1810.2.el7.centos.x86_64
[vagrant@localhost ~]$
```

Adapter 1: Intel PRO/1000 MT Desktop (NAT)
Adapter 2: Intel PRO/1000 MT Desktop (Host-only

USB: Disabled

Shared Folders: 1

Installed with Vagrant:

```
Vagrant.configure("2") do |config|
  (1..3).each do |i|
    config.vm.define "Centos#{i}" do |ubuntu|
      ubuntu.vm.box = "geerlingguy/centos7"
     end
  end
end
```

2. Configure VMs:

About IPtables https://wiki.centos.org/HowTos/Network/IPTables
Networks types in Virtual box

Network type	Access Guest -> other Guests	Access Host -> Guest	Access Guest -> external Network
Not attached	-	-	-
Network Address Translation (NAT)	-	-	✔
Network Address Translation Service	✔	-	✔
Bridged networking	✔	✔	✔
Internal networking	✔	-	-
Host-only networking	✔	✔	-

Configuration of VM's adapters:
Nat network = 192.168.133.0/24
10.0.2.15 - access to Internet

VM#1	Adapter#1			Adapter#2			Adapter#3		
	Name	Type	IP address	Name	Type	IP address	Name	Type	IP address
1	enp0s3	NAT	10.0.2.15	enp0s8	NAT network	192.168.133.11	enp0s9	Host only	192.168.56.180
2				enp0s8	NAT network	192.168.133.12	enp0s9	Host only	192.168.56.181
3				enp0s8	NAT network	192.168.133.13	enp0s9	Host only	192.168.56.182

VM1

- **must have connection to Public Internet via own nat interface**
- **must be available for VM2,VM3 via host-only interface**

VM1, ifcfg-enp0s3

```
TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=dhcp
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
NAME=enp0s3
DEVICE=enp0s3
UUID=88cc6876-bdf7-4f97-94de-134e4453db2
ONBOOT=yes
DNS1=8.8.8.8
DNS2=8.8.4.4
```

VM1, ifcfg-enp0s8

```
TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=static
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
NAME=enp0s8
DEVICE=enp0s8
UUID=a36d275b-5eca-40cb-9fda-300eb51b8a78
ONBOOT=yes
IPADDR=192.168.113.11
NETMASK=255.255.255.0
```

VM1, ifcfg-enp0s9

```
This file doesn’t exist, looks like Virtual box manage host-only configured
adapters without config file
```

VM2

- **must have access to Public internet via nat interface of VM1**
- **must be available for VM1,VM3 via host-only interface**

VM2, ifcfg-enp0s8

```
TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=static
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
NAME=enp0s8
DEVICE=enp0s8
UUID=a36d275b-5eca-40cb-9fda-300eb51b8a78
ONBOOT=yes
IPADDR=192.168.113.12
NETMASK=255.255.255.0
GATEWAY=10.0.2.15
```

VM2, ifcfg-enp0s9

```
This file doesn’t exist, looks like Virtual box manage host-only configured
adapters without config file
```

VM3

- **must be available for VM1,VM2 via host-only interface**
- **no access to Public Internet**

VM3, ifcfg-enp0s8

```
TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=static
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
NAME=enp0s8
DEVICE=enp0s8
UUID=a36d275b-5eca-40cb-9fda-300eb51b8a78
ONBOOT=yes
IPADDR=192.168.113.13
NETMASK=255.255.255.0
GATEWAY=10.0.2.15
```

VM3, ifcfg-enp0s9

```
This file doesn’t exist, looks like Virtual box manage host-only configured
adapters without config file
```

3. Send your network configuration via email:

- **ifcfg-enp0s3 and if-cfg-enp0s8 from each VM (6 files)**
- **iptables/firewall-cmd rules' list (1 file) and commands, which were used for**
- **iptables/firewall-cmd configuration (as text in email)**

Now we need to create rules which direct TCP packages from VM2,VM3 to VM1 enp0s3 adapter and to internet. Packages from VM should be enabled, from VM3 should be disabled

Centos 7 use firewalld. I prefer use iptables:

```
systemctl disable firewalld
yum install iptables-services
systemctl enable iptables
systemctl start iptables
sysctl -w net.ipv4.ip_forward=1  # enable FORWARDing
```

Iptables rules is saved in file `/etc/sysconfig/iptables`
Rules should be manually saved by command:
`service iptables save`

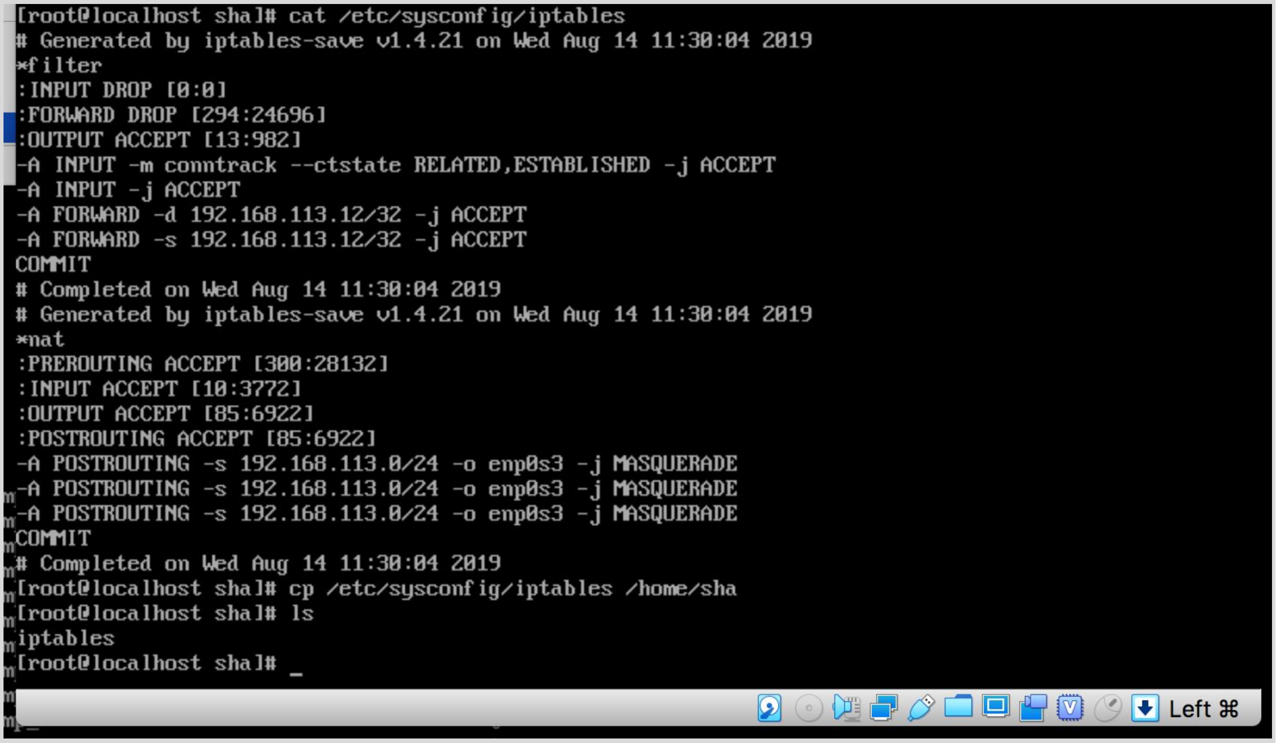
Config iptables:

```
iptables -F
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT ACCEPT # for any case

# allow package with status related, established pass through INPUT chain
iptables -A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT

#allow NAT 192.168.133.0/24 connect with internet
iptables -A POSTROUTING -t nat -s 192.168.133.0/24 -o enp0s3 -j MASQUERADE

#allow VM2 transfer through chain FORWARD
iptables -A FORWARD -d 192.168.113.12 -j ACCEPT
iptables -A FORWARD -s 192.168.113.12 -j ACCEPT
```

Result file `/etc/sysconfig/iptables`

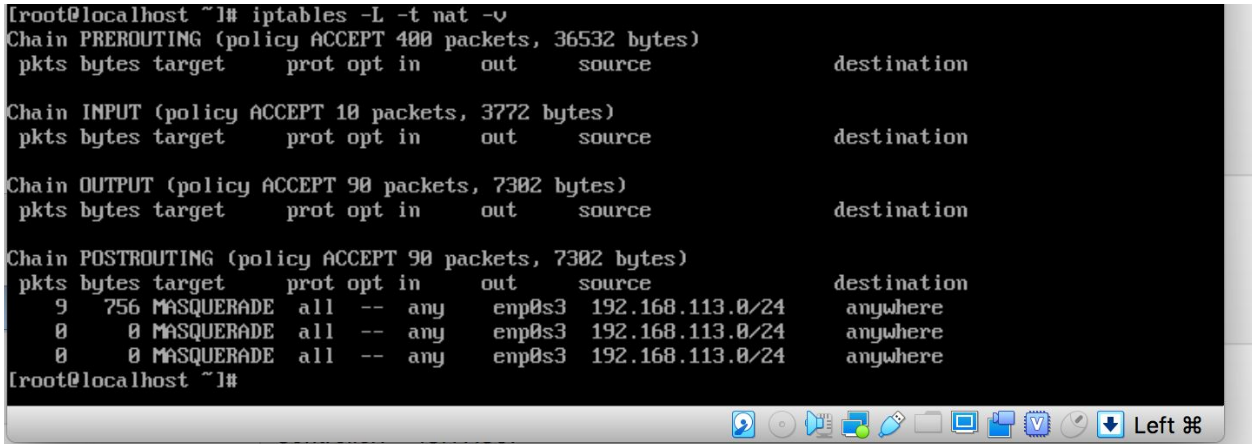
```
# Generated by iptables-save v1.4.21 on Wed Aug 14 11:30:04 2019
* filter
:INPUT DROP [294:24696]
:OUTPUT ACCEPT [13:982]
-A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -d 192.168.113.12/32 -j ACCEPT
-A FORWARD -s 192.168.113.12/32 -j ACCEPT
COMMIT
# Completed on Wed Aug 14 11:30:04 2019
# Generated by iptables-save v1.4.21 on Wed Aug 14 11:30:04 2019
*nat
PREROUTING ACCEPT [300:28132]
INPUT ACCEPT [10:3772]
OUTPUT ACCEPT [85:6922]
POSTROUTING ACCEPT [85:6922]
-A POSTROUTING -t nat -s 192.168.133.0/24 -o enp0s3 -j MASQUERADE
COMMIT
# Completed on Wed Aug 14 11:30:04 2019
```

file `/etc/sysconfig/iptables`



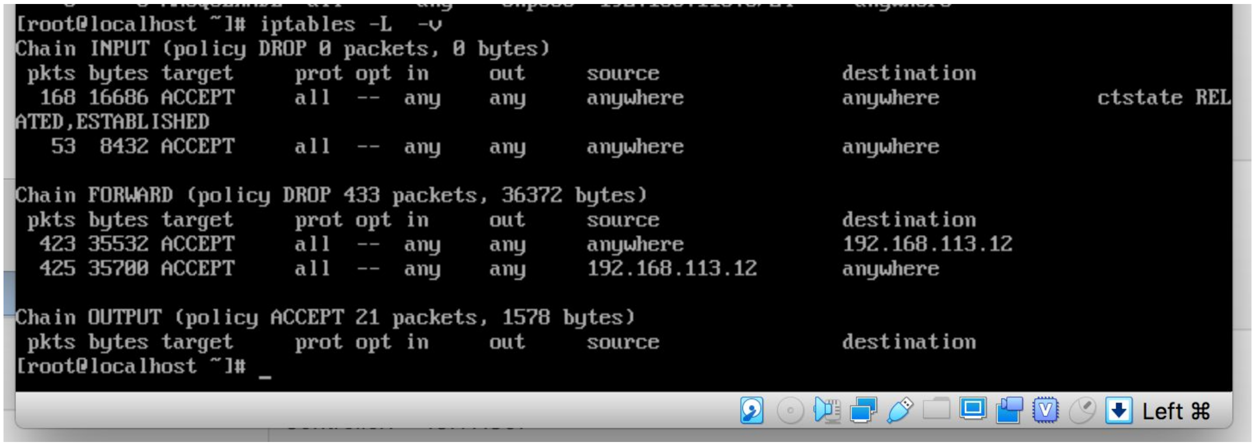
```
[root@localhost sha]# cat /etc/sysconfig/iptables
# Generated by iptables-save v1.4.21 on Wed Aug 14 11:30:04 2019
*filter
:INPUT DROP [0:0]
:FORWARD DROP [294:24696]
:OUTPUT ACCEPT [13:982]
-A INPUT -m comntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A INPUT -j ACCEPT
-A FORWARD -d 192.168.113.12/32 -j ACCEPT
-A FORWARD -s 192.168.113.12/32 -j ACCEPT
COMMIT
# Completed on Wed Aug 14 11:30:04 2019
# Generated by iptables-save v1.4.21 on Wed Aug 14 11:30:04 2019
*nat
:PREROUTING ACCEPT [300:28132]
:INPUT ACCEPT [10:3772]
:OUTPUT ACCEPT [85:6922]
:POSTROUTING ACCEPT [85:6922]
-A POSTROUTING -s 192.168.113.0/24 -o enp0s3 -j MASQUERADE
-A POSTROUTING -s 192.168.113.0/24 -o enp0s3 -j MASQUERADE
-A POSTROUTING -s 192.168.113.0/24 -o enp0s3 -j MASQUERADE
COMMIT
# Completed on Wed Aug 14 11:30:04 2019
[root@localhost sha]# cp /etc/sysconfig/iptables /home/sha
[root@localhost sha]# ls
iptables
[root@localhost sha]# _
```

Table nat



```
[root@localhost ~]# iptables -L -t nat -v
Chain PREROUTING (policy ACCEPT 400 packets, 36532 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain INPUT (policy ACCEPT 10 packets, 3772 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 90 packets, 7302 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain POSTROUTING (policy ACCEPT 90 packets, 7302 bytes)
 pkts bytes target     prot opt in     out     source               destination
    9   756 MASQUERADE  all  --  any    enp0s3  192.168.113.0/24     anywhere
    0     0 MASQUERADE  all  --  any    enp0s3  192.168.113.0/24     anywhere
    0     0 MASQUERADE  all  --  any    enp0s3  192.168.113.0/24     anywhere
[root@localhost ~]#
```

Table filter



```
[root@localhost ~]# iptables -L  -v
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
  168 16686 ACCEPT     all  --  any    any     anywhere             anywhere             ctstate REL
ATED,ESTABLISHED
   53  8432 ACCEPT     all  --  any    any     anywhere             anywhere

Chain FORWARD (policy DROP 433 packets, 36372 bytes)
 pkts bytes target     prot opt in     out     source               destination
  423 35532 ACCEPT     all  --  any    any     anywhere             192.168.113.12
  425 35700 ACCEPT     all  --  any    any     192.168.113.12       anywhere

Chain OUTPUT (policy ACCEPT 21 packets, 1578 bytes)
 pkts bytes target     prot opt in     out     source               destination
[root@localhost ~]# _
```