



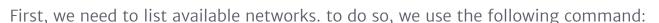
Mohammed Aboullaite | 26 Nov 2017 | 3 min (757 words)

KVM/libvirt: Forward Ports to guests with Iptables

I've been playing in the past few weeks with kvm/qemu and libvirt to set up some VMs. If you've been using libvirt before, you'll for sure agree that <u>Libvirt</u> is particularly awesome when it comes to managing virtual machines, their underlying storage and networks. However, if you happen to use <u>NAT-ed networking</u> and want to allow external access to services offered by your VMs, you've got to do some manual work. In this post, I'll try to demystify the process of NAT port forwarding to VMs.



static IP address to VM



1 2	<pre>\$ virsh net-list Name</pre>	State	Autostart	Persistent	
3 4	xhubnet	active	yes	yes	

To see the xhubnet network information:

- 4 <uuid>2ba36c4f-46c9-4767-a9fc-6808cf001a19</uuid>

```
<forward mode='nat'>
             <nat>
 6
 7
             <port start='1024' end='65535'/>
             </nat>
 8
9
         </forward>
         <bridge name='virbr1' stp='on' delay='0'/>
10
         <mac address='52:54:00:8e:b5:88'/>
11
         <domain name='xhubnet'/>
12
         <ip address='192.168.111.1' netmask='255.255.255.0'>
13
14
             <dhcp>
             <range start='192.168.111.120' end='192.168.111.254'/>
15
             </dhcp>
16
         </ip>
17
         </network>
18
```

Where it's clearly indicated that the DHCP range is between 192.168.111.120 and 19 111.254.

first step toward setting up a public IP to our VM, is to get it MAC addresses and this is easy to achieve using virsh CLI:

```
1     $ virsh dumpxml VM_NAME | grep -i '<mac'
2     <mac address='52:54:00:e2:95:c6'/>
```

The last step is to edit the network config to add new VM config using the following command:

```
1 $ virsh net-edit xhubnet
```

and add this line after the <range ...> section:

```
1 <host mac='52:54:00:e2:95:c6' name='VM_NAME' ip='192.168.111.36'/>
```

To make changes effective, we need to start DHCP service using:

```
1  $ virsh net-destroy xhubnet
2  $ virsh net-start xhubnet
```

Restarting DHCP service should be enough, However in some cases you need to restart the libvirt-bin service:



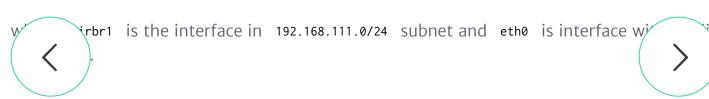
Configuring the Firewall to port forward

By default, guests that are connected via a virtual network with <forward mode='nat'/> can make any outgoing network connection they like. Incoming connections are allowed from the host, and from other guests connected to the same libvirt network, but all other incoming connections are blocked by iptables rules.

If we would like to make a service that is on a guest behind a NATed virtual network publicly available, we need to setup the necessary iptables rules to forward incoming connections to the host on any given port.

Let's suppose for example that we need to forward the forward incoming connections to port 9867 on host machine to port 22 on guest machine. below are the needed rules to achieve that:

```
# connections from outside
 1
         $ iptables -I FORWARD -o virbr1 -d 192.168.111.36 -j ACCEPT
 2
 3
         $ iptables -t nat -I PREROUTING -p tcp --dport 9867 -j DNAT --to 192.168.111.
         # Masguerade local subnet
 5
         $ iptables -I FORWARD -o virbr1 -d 192.168.111.36 -j ACCEPT
 6
 7
         $ iptables -t nat -A POSTROUTING -\mathbf{s} 192.168.111.0/24 -\mathbf{j} MASQUERADE
         $ iptables -A FORWARD -o virbr1 -m state --state RELATED, ESTABLISHED -j ACCEF
         $ iptables -A FORWARD -i virbr1 -o eth0 -j ACCEPT
9
         $ iptables -A FORWARD -i virbr1 -o lo -j ACCEPT
10
```



Now that we have set up port forwarding, we can save this to our permanent rule set and load the rule set:

```
1  $ service netfilter-persistent save
2  $ service netfilter-persistent reload
```

Now, test that your VM is accessible through your firewall's public IP address:

```
1 $ ssh user@PUBLIC_IP -p 9867
```

This should work!