

Network containing

To limit a KVM guest to only reach one specific gateway, you must block all other traffic using iptables or nftables on the Linux host. Because virt-manager does not have a built-in button for this, the cleanest way is to use a libvirt hook script. This script automatically applies network restrictions every time the VM starts.

Step 1: Find your VM's network interface

Run this command on your host to find the virtual interface name while the VM is running:

```
# virsh domiflist <Your-VM-Name>
```

Note the Interface name (e.g., vnet0 or vnet1).

Step 2: Create a Libvirt hook script

Libvirt can execute scripts when VMs start. We will use a qemu hook to isolate the traffic.

Open a terminal on your host and create the hook directory if it does not exist.

```
# mkdir -p /etc/libvirt/hooks
```

Create and edit the hook file.

```
# /etc/libvirt/hooks/qemu
```

Paste the following script (replace vnet0 and 192.168.122.1 with your actual interface and allowed gateway):

```
#!/bin/bash

VM_NAME="Your-VM-Name"
INTERFACE="vnet0"
ALLOWED_GATEWAY="192.168.122.1"

OBJECT=$1
OPERATION=$2
if [ "$OBJECT" = "$VM_NAME" ]; then
    if [ "$OPERATION" = "started" ] || [ "$OPERATION" = "start" ]; then
        # 1. Allow traffic to the specific gateway IP
        iptables -I FORWARD -m physdev --physdev-in $INTERFACE -d
$ALLOWED_GATEWAY -j ACCEPT
        iptables -I FORWARD -m physdev --physdev-out $INTERFACE -s
$ALLOWED_GATEWAY -j ACCEPT
```

```
# 2. Drop all other traffic from this interface
iptables -A FORWARD -m physdev --physdev-in $INTERFACE -j DROP
iptables -A FORWARD -m physdev --physdev-out $INTERFACE -j DROP
fifi
```

Step 3: Make the script executable and restart libvirt

Make the script executable:

```
# chmod +x /etc/libvirt/hooks/qemu
```

Restart the libvirt service to load the new hook:

```
# systemctl restart libvirtd
```

Now, every time you start this specific VM, the host firewall will block all network traffic unless it is explicitly sent to or from your chosen gateway IP. If you are using nftables instead of iptables, or if you need help finding the exact subnet/gateway IP of your virt-manager network, let me know!

From:
<https://wiki.oscardegroot.nl/> - HomeWiki

Permanent link:
<https://wiki.oscardegroot.nl/doku.php?id=linux:apps:kvm:kvm-hardening&rev=1789281312>

Last update: **2026/09/13 06:35**

