Firewalling virtuals with ebtables

I had a situation where I wanted to control access from one virtual to the others on the network. It could have been done via NAT, but the eventual goal is to have several virtual machines which can not “see” each other, and did now want to go building several virtual networks. So, I researched ebtables.

ebtables (http://ebtables.netfilter.org/) is a network filtering tool designed to work with Unix Bridges. Most (all?) virtualization software supports, and even recommends, using a network bridge.

Since a bridge forwards, the filtering is done under the FORWARD rule.

In this example, we are looking at three machines:

Name	MAC	Description
Win10	00:16:3e:6b:26:70	this is the machine we want to restrict
router	00:16:3e:bd:26:71	this is the router
manage	00:16:3e:37:26:72	this is the one internal machine which may be reached

Win10 is a *virtual* inside our network. We need to be able to access it from *manage*, and also it needs to access the Internet via *router*. We also want to access *Win10* via RDP over VPN. However, *Win10* should not 'see' anything else on our network.

ebtables works with MAC addresses, so we track the MAC's. The above MAC's are samples randomly chosen from those assigned for some forms of virtualization; use your own MAC addresses.

Basically, we add rules to allow access between *Win10* and *router*, and *Win10* and *manage*, then we add rules to not allow any other access.

Not sure why, but we need protocols 0x800 and 0x806 (IPv4 and ARP) specifically allowed to the router or this will not work. You can still access from *manage* but not over a VPN connection. Still researching that.

```
# first, flush all tables (restore to default)
ebtables -F
# let Win10 talk to router
ebtables -A FORWARD -s 00:16:3e:6b:26:70 -d 00:16:3e:bd:26:71 -j ACCEPT
# let router talk to Win10
ebtables -A FORWARD -s 00:16:3e:bd:26:71 -d 00:16:3e:6b:26:70 -j ACCEPT
# let Win10 talk to manage
ebtables -A FORWARD -s 00:16:3e:6b:26:70 -d 00:16:3e:37:26:72 -j ACCEPT
# let manage talk to Win10
ebtables -A FORWARD -s 00:16:3e:37:26:72 -d 00:16:3e:6b:26:70 -j ACCEPT
# not sure why, but we need these two protocols usable
ebtables -A FORWARD -s 00:16:3e:6b:26:70 -p 0x800 -j ACCEPT
ebtables -A FORWARD -s 00:16:3e:6b:26:70 -p 0x806 -j ACCEPT
# Drop all other traffic where Win10 is the source
ebtables -A FORWARD -s 00:16:3e:6b:26:70 -j DROP --log
# and drop all other traffic where Win10 is the destination
```

```
ebtables -A FORWARD -d 00:16:3e:6b:26:70 -j DROP --log
# show the user what the tables look like.
ebtables -L
```

Links

1. https://superuser.com/questions/423276/what-does-type-ip-0x0800-in-the-ethernet-ii-part-of-a-ping-packet-mean
2. https://community.broadcom.com/symantecenterprise/communities/community-home/digestviewer/viewthread?MessageKey=39fec5ae-d06b-4c65-8b26-da0b35f530fc
3. https://sbarjatiya.com/notes_wiki/index.php/Basic_ebtables_configuration
4. http://ebtables.netfilter.org/
5. https://linux.die.net/man/8/ebtables