# Ubuntu Firewall

[Ubuntu Firewall 1](#_Toc207571532)

[Virtual Machine Setup: 2](#_Toc207571533)

[Configuration and Testing: 4](#_Toc207571534)

[Setup Vlan for Firewall: 4](#_Toc207571535)

[Netplan Example 4](#_Toc207571536)

[Apply Netplan: 5](#_Toc207571537)

[Enable routing and Nat: 5](#_Toc207571538)

[Iptables Rules 5](#_Toc207571539)

[Saving Iptables Rules: 6](#_Toc207571540)

[Netplan Functioning: 6](#_Toc207571541)

## Virtual Machine Setup:

Start by installing and creating a baseline ubuntu server vm (update\_password)

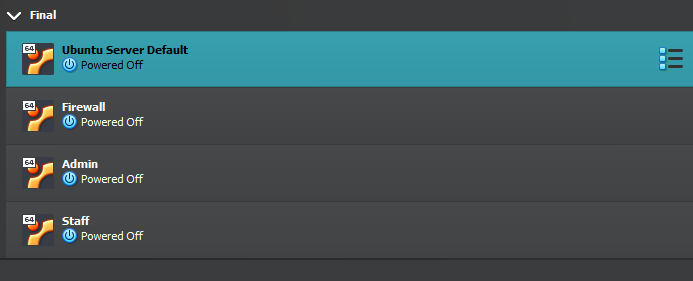


Clone 7 times and put in a group for visual clarity. Generate new mac for each and make sure they are full clones.

This is the Nic Setup for the VMS:

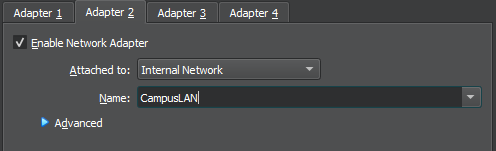
**Firewall:** Server NAT Nic 1, Internal Network Nic 2

**Vlan Vms:** Internal Network Nic 1

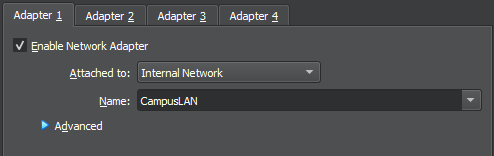


For testing basics these 3 will do.

Firewall Vm Nic 1 Nat and Nic 2 Internal



Vlan Vms Nic 1 Internal



## Configuration and Testing:

### Setup Vlan for Firewall:

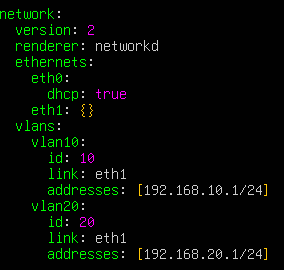
sudo apt update

sudo apt install vlan

sudo modprobe 8021q

echo "8021q" | sudo tee -a /etc/modules

Netplan Example (see Teams and Github for all)



Use Alt P to show whitespace.

Apply Netplan: sudo netplan apply

### Enable routing and Nat:

echo "net.ipv4.ip\_forward=1" | sudo tee -a /etc/sysctl.conf

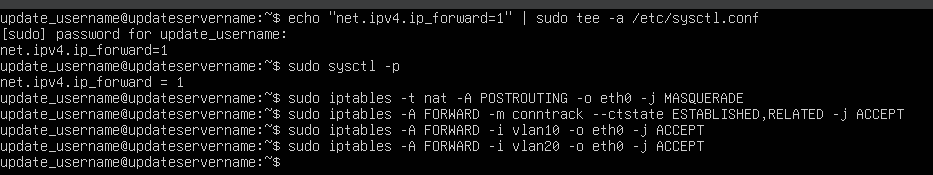
sudo sysctl -p

sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

sudo iptables -A FORWARD -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

sudo iptables -A FORWARD -i vlan10 -o eth0 -j ACCEPT

sudo iptables -A FORWARD -i vlan20 -o eth0 -j ACCEPT



Was utilizing incorrect interface names. This has been remedied by running the command ip-a to get the correct interface names and rewrite the netplan rules and ip tables based of that.

### Iptables Rules

*Enable NAT for Internet access via uplink*

sudo iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE

*Allow established/related traffic back in*

sudo iptables -A FORWARD -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

*Allow VLAN10 and VLAN20 out to Internet*

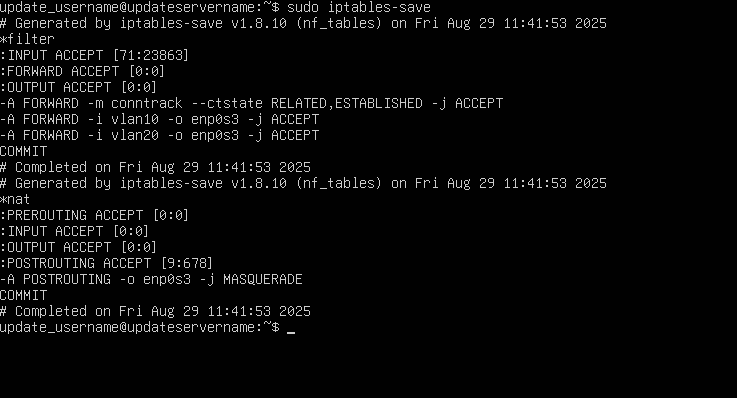
sudo iptables -A FORWARD -i vlan10 -o enp0s3 -j ACCEPT sudo iptables -A FORWARD -i vlan20 -o enp0s3 -j ACCEPT

### Saving Iptables Rules:

sudo apt install iptables-persistent

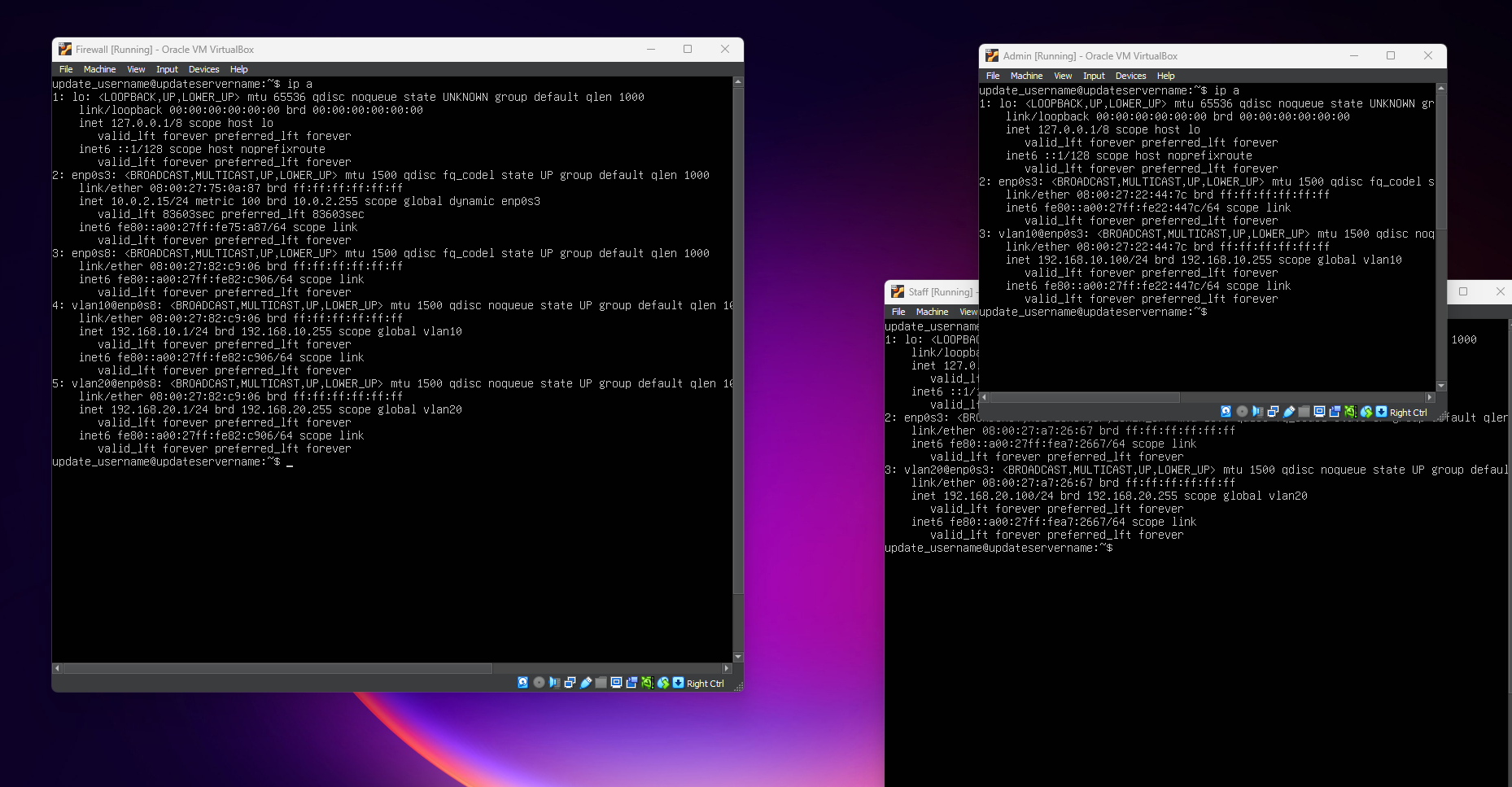
sudo netfilter-persistent save

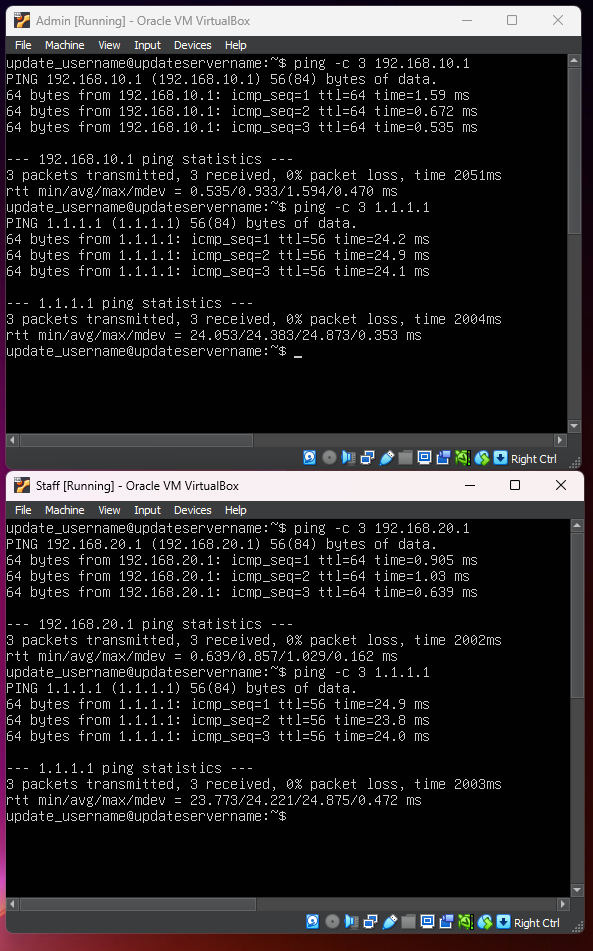
Sudo iptables-save to see full saved iptables



### Netplan Functioning:

On firewall 03, 08, 10, 20 | On admin 10 | On staff 20





Firewall Vlan10

Internet test via firewall

Firewall Vlan20

Internet test via firewall

See Video Working Vlan Iptables for proof of iptables effecting the vlans allowing them to and not to communicate with each other.

TODO:

Add the other vms and after that access control.