Network namespace

To provide additional kernel network namespace to use for virtualization. Create dev machines to have the same range of ip address with prod machines. They are running on the same machines but they never communicate with each other.

# Sudo ip netns add development

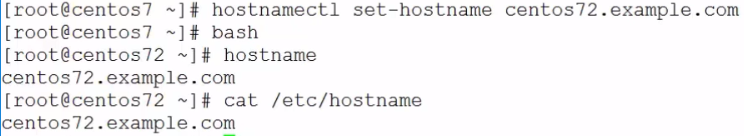
# Ip netns

HOSTNAME

Uname –n = show nodename

Hostnamectl – to show full information about name

This is to change hostname . This change sets it in the tranion, memory residence and configuration file



To check pretty name

Cat /etc/machine-info

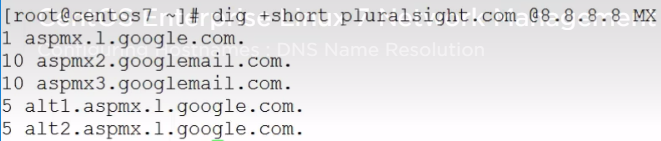
NAME RESOLUTION

Cat /etc/resolv.conf

To be able to use dig utilities to test resolution = yum install –y bind-utils

Dig [www.pluralsight.com](http://www.pluralsight.com) @8.8.8.8

Dig +short [www.pluralsight.com](http://www.pluralsight.com) @8.8.8.8



This shows the priority, the order at which the mail exchange will be used, the lower the number the more likely it is going to be used.

NS = The order of resolution is controlled through the name server switch file

**Yum install Avahi –y** = you can go out on the network and look for hostname that are been advertised on multicast DNS. Makes it easy to connect to hosts that are on the same network that you are connected to.

NTP

Date – displays the system time

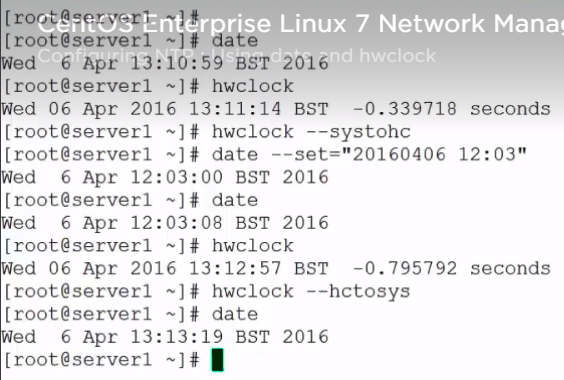
Hwclock – displays real time clock hardware clock

hwclock –systohc = To synchronize both above

Hwclock --hctosys = synch your hardware close to your system time

Timedatectl set-data = use this to set hardware clock and system time

timedatactl



To change time in our hardware clock and memory resident or system time

Timedatectl set-time “2016-04-06 13:30:00” = to make this work, time synchronization cannot be enabled.

Timedatectl set-ntp false

CHRONY

Yum install –y chrony

Vim /etc/chrony.conf = configure file

Systemctl enable chrony ; systemctl start chrony

Chronyc tracking

Ntpq –p = check the synchronization status

**NETWORKING**

Ip addr show OR ip a OR ip -4 a= check ip address

**127**.0.0.1/8 = The first block of numbers represent the network and the last 3 represents the host

Enp0S3 = This is pci box 0 and slot 3. It is the representative of the network card

**10.0.2**.21/24 = The first 24 bits makes up the network and the last 8 makes up the host

Ip -4 a s enp0s8 = This is showing only one interface

**NETWORK MANAGER**

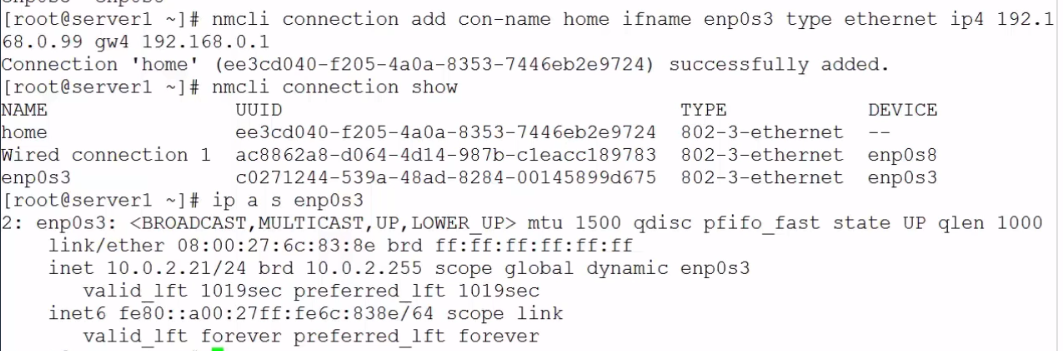
These are default service that manages out network connectivity.

Systemctl status NetworkManager

To list out connections

# Nmcli connection show = You can double click TAB to show more

# Nmcli –p connection show = pretty format

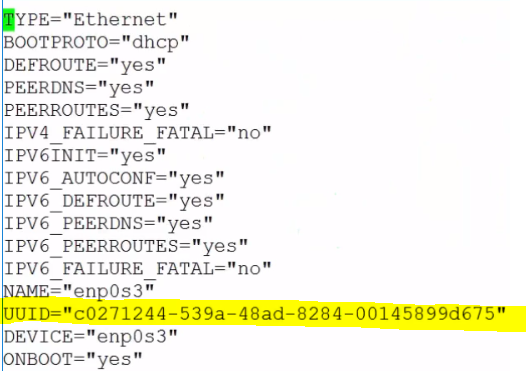


# nmcli con down

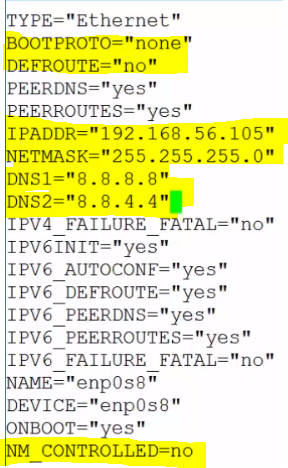
# nmcli con up

Then repeat IP show command

# ip a s enp0s3

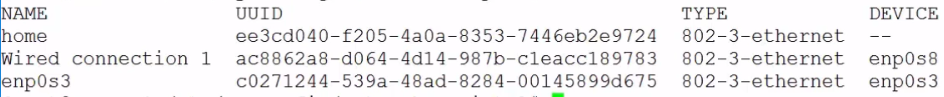


Add items in yellow



If you do not want the network manager to be controlled, change NM\_CONTROLLED=no to yes

/etc/sysconfig/network-scripts



Nmcli con delete wired conection

# ifdown enp0s8

# ifup enp0s8

# systemctl stop NetworkManager.service

# systemctl start networkManager.service

**ROUTING**

Route table contains a list of network that each host knows about. It include independent network as long as the dault route.

Ip route show - to see your route table

Route | netstart –r | netstat –rn | ip r

We have 2 routers and one has network. If you want to connect to the world, you have to use the server 2 router.so we enable server 2 to be the default gate way for server 1, on server1 host, enter the below

# ip route add default via ipadsofserver2

# vim /etc/sysctl.cnfd 🡪 net.ip4 v4.ip\_forward=1

Sysctl -p

We can enable roube on serhttps://equifax.gr8people.com/index.gp?method=cappportal.showJob&sysLayoutId=122&opportunityId=19454ver2, this is done through proc file system.

Vi /etc/sysctl.conf

Net.ipv

You can use this new default as a gateway on the server. Go on the network interface card and turn DEFROUTE ‘’NO” to “YES”

Cat /proc/sys network configifuration file

**NAT**

We need to enable network access translation. This are used to provide access to private networks

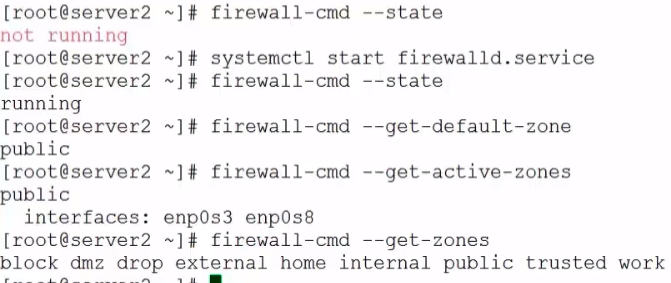
# Ipables –L = This shows you input and out

To enable NAT translation

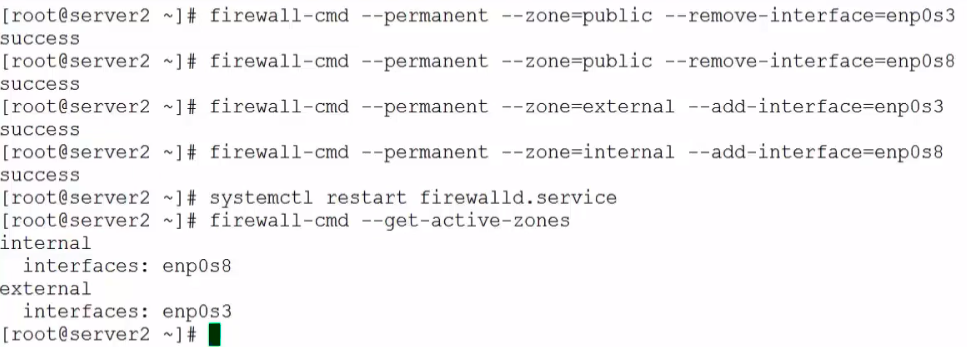
# Iptables –t nat –A POSTROUTING \ -o enp0s3 –j MASQUERADE

**FIREWALLD**

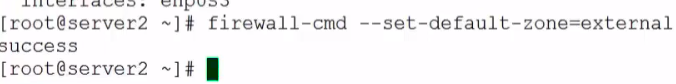
Anytime we add a new service, we have to open a firewall or close it. The purpose of firewall is to retrict access to services by controlling their potes



To change zones from public zone



You can also set the default zone. We should be more interested in the external zone

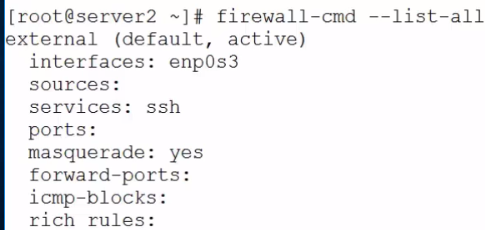


SERVICE RULES & PORTS RULES

# firewall-cmd --list-all

Firewall-cmd --list-all --zone=internal

# firewall-cmd --list-all --zone=public



From the above, external has been set as default so when you run--list-all, external is what will pop up

* We have to turn off SSH as we do not want it public. To turn SSH off

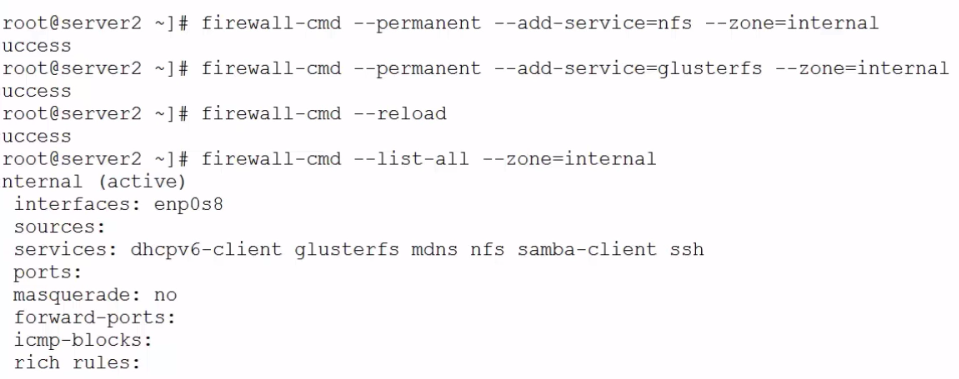
# firewall-cmd --permanet --remove-service=ssh

# firewall-cmd –reload = this will allow any changes to take effect

Now you notice ssh is gone

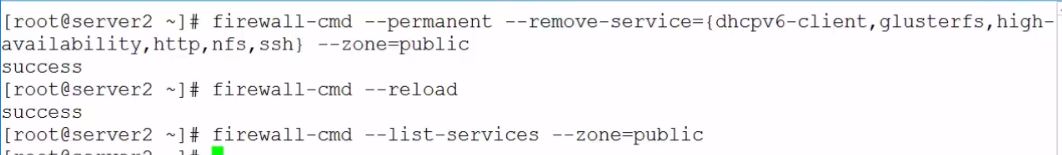
* Let’s look at the internal zones

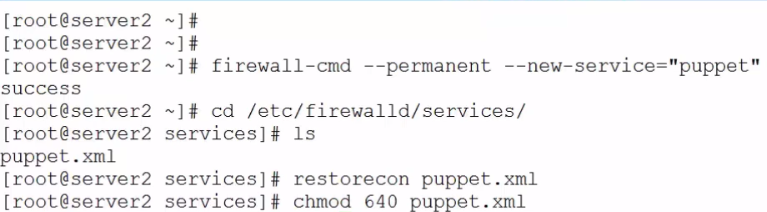
# Firewall-cmd—list-all --zone=internal



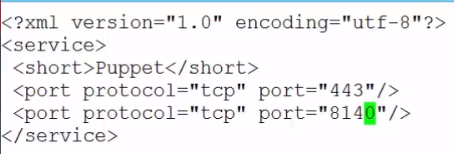
More settings

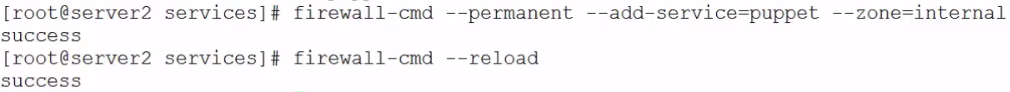






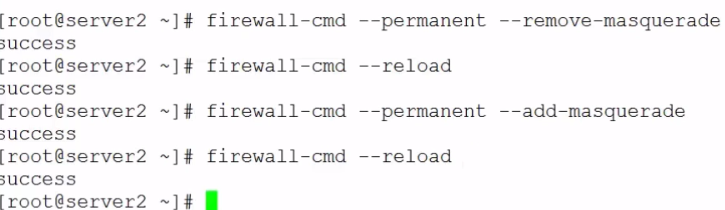
Vi puppet.xml

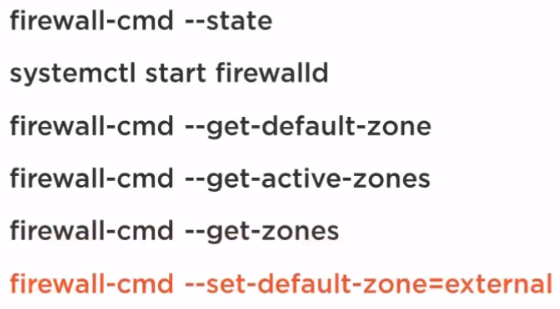


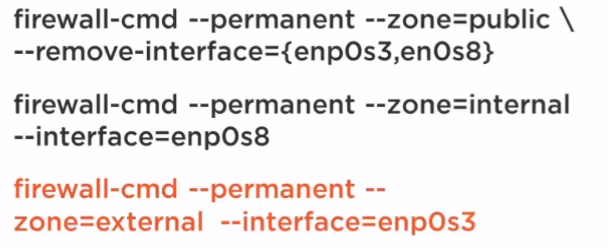


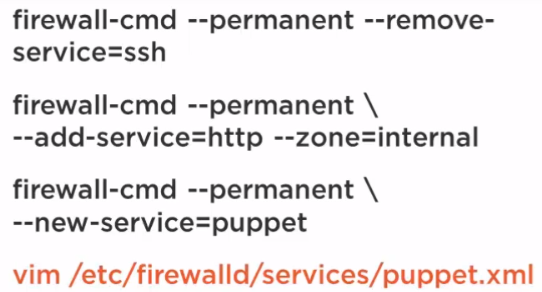
**NAT and Masquerades**

IP masquerading is a form of network address translation (NAT) which allows internal computers with no known address outside their network, to communicate to the outside. It allows one machine to act on behalf of other machines.







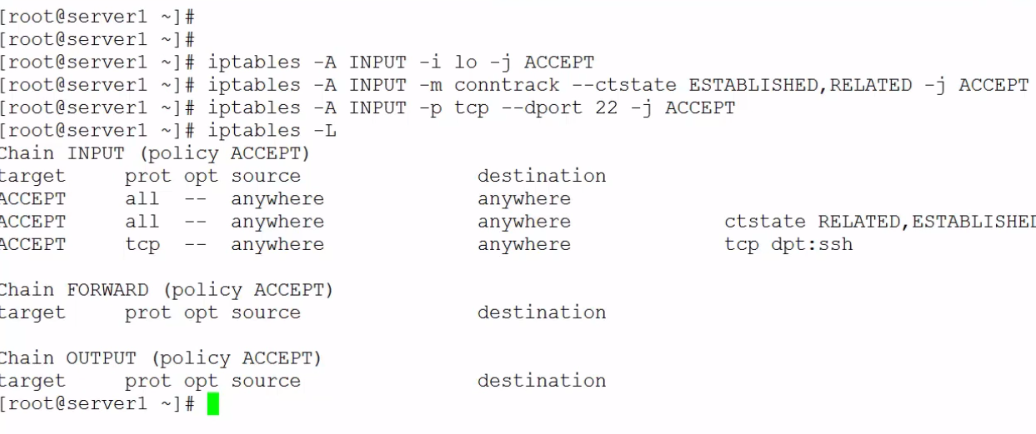


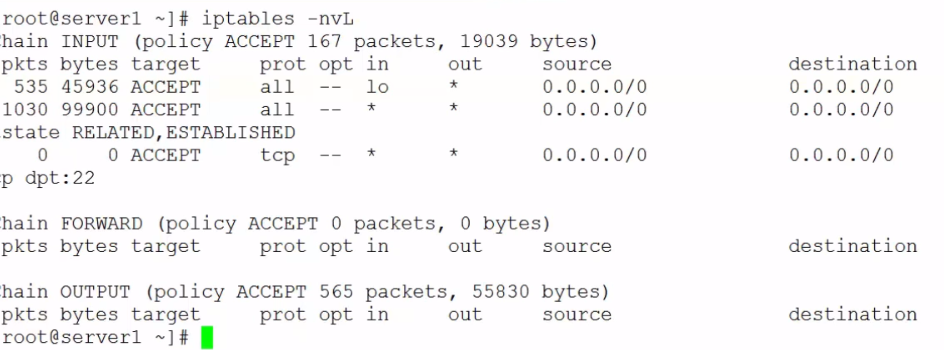
**IPTABLES**

Iptables –L = This lists the default table

Before editing you need to save the configuration of the iptables so if you have to read the configuration later, you can.

# Iptables-save > fwoff

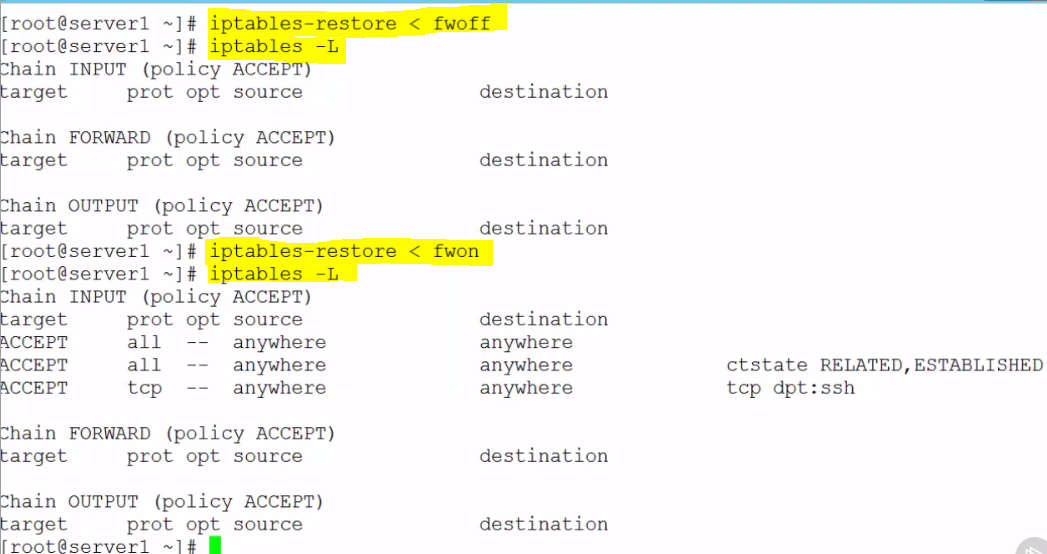




Iptables-save > fwon = we are saving our configuration to the onfile

Now read file = iptables -L

Iptables-restore < fwoff = we are reading from the fwoff, you will not see new rules



Anytime you want to make changes to the file, you input the on configuration

Iptables-save < fwon

And when complete, you can re-add

Iptables-save > fwon

Iptables –F 🡪 This is to flush the rules

You can edit fwon anytime;

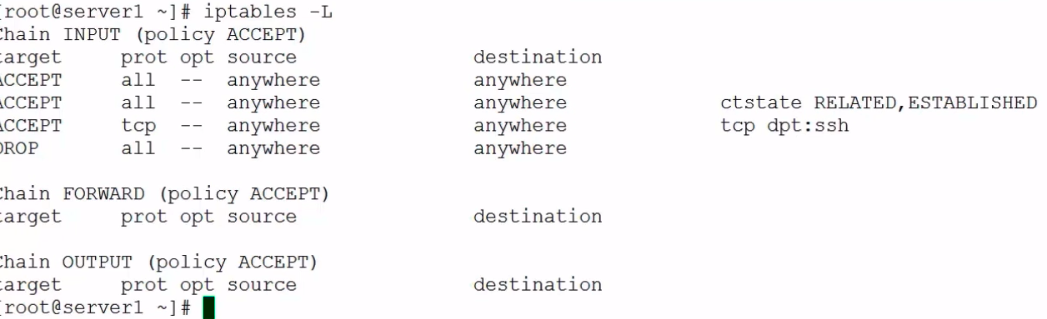
# -A INPUT –J DROP = if it has not matched the rule, then drop packet. Only previously matched rule should stay

Iptables<restore < fwon

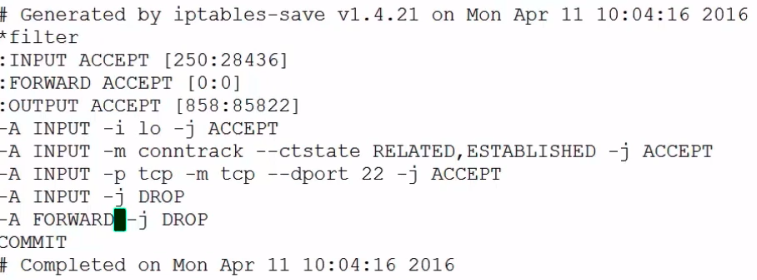
Note: We are saving iptables to fwon so we can also input the rule to the iptables if anything happens

**FIREWALL DESIGN**

Let us look at the accept policy for INPUT, FORWARD AND OUTPUT. It is better to leave the ACCEPT and then drop at the last rule



Vi fwon



Save and exit

Iptables-restore < fwon

**INSTALL IP TABLES SERVICES**

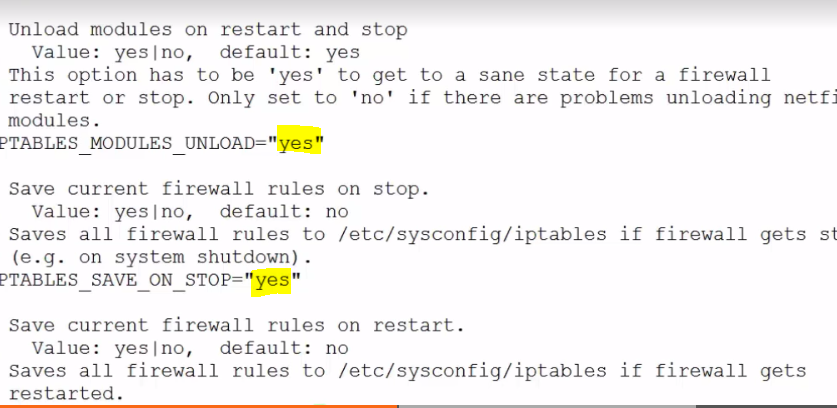
Here we will see how we can use IP tables as a service on centos7

Yum install –y iptables-services

Vi /etc/sysconfig/iptables

Vi /etc/sysconfig/iptables-config

Change in the highlighted below from no to yes.



Disable firewalld.services and start iptables

To open port



Restart iptables

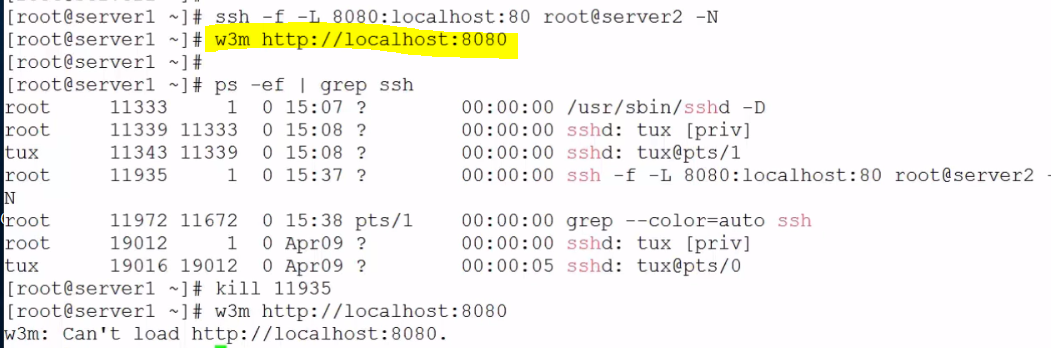
**METHODS TO TUNNEL TRAFFIC**

**CREATING SSH TUNNL**

W3m localhost = get into your webserver on your local host

**Ssh –f -L 8080:localhost:\:80 root@server2 –N**

**W3w** [**http://localhost.com**](http://localhost.com)



INSTALL OPEN VPN SERVER

Yum install openvpn easy-rsa -y

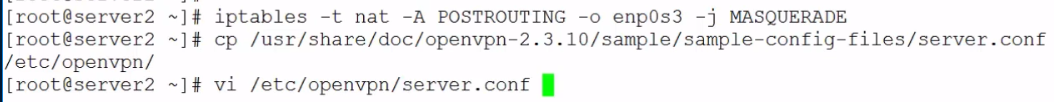
Systemctl stop firewalld

# iptables –L

To double chek – iptables –L –t nat

Add masquerade

Iptables –t nat –A POSTROUTING –o enp0s3 –J MAQUERADE



Now you configure the certificate

Uncomment push “redirect-gateway def1 bypass-dcp”

Add google dns

Push “dhcp-options DNS8.8.8.8”

Push “dhcp-options DNS8.8.8.8”

Save and exit



\*\*configuring an open VPN Server

\*\*configuring an open VPN Client

\*\*Connecting to the open VPN server

**MONITOR THE NETWORK**

**TRACEPATH**

You can use this to check that you are following the right path/route on the internet

**#** tracepath [www.pluralsight.com](http://www.pluralsight.com)

DISPLAY NETWORK STATISTICS WITH IP

Helps to retrieve info such as mark address

# Ip -4 a s

Ip link show

Ip –s link show enp0s8 = shows statistics on an interface

Where RX – is received bytes

TX – Transmitted bytes

# netstat –tln

This show you tcp ports number and if it is listening instead of showing name

# netstat –I = show you receive and transmit data

Shows you interfaces . we can see the highest use on the top

# netstat –s = shows you the complete IP stack

This will show you stack statistics

SYSSTAT

This collects information every 10 mins. It shows Memory utilization, disk utilization

# systat

# ls /etc/cron.d

# ls /var/log/sa

To read files

# sar –n DEV OR # sar -n DEV 1 1

NAMP

This is used to check ports that are opened.

# nmap scanme.nmap.org

# nmap –iflist

You can use this to document your system. It shows you are list of your IP’s, network and route tables