Setting up a CentOS Router

> **Note**
>
> This tutorial will cover setting up a firewalld firewall and making your system a router. firewalld is preinstalled on CentOS and Red Hat Enterprise Linux systems.

Introduction

To follow the contents of this tutorial, be sure to follow inside a terminal. Most operations require super user priviliges. For the sake of the tutorial, be sure all commands are executed as root or execute all commands with sudo.

Editor

Replace any instances of vi with your command-line editor of choice. Possible editors include:

- vi
- nano

Instructions

Any areas where ${} appears means it is a replaceable variable. Replace the whole text, including ${} with your text.

Below are the variables that will be used throughout the guide.

Variable	Value
${EXTERNAL_IP}	172.18.13.t
${EXTERNAL_NETMASK}	255.255.0.0
${EXTERNAL_GATEWAY}	172.18.0.1
${EXTERNAL_DNS}	172.18.0.12
${INTERNAL_IP}	192.168.t.1
${INTERNAL_GATEWAY}	255.255.255.0
${NETMASK}	24

> **Note**
>
> Replace any instances of t with your team number. Alternatively, for a private setup, just use 1 for simplicity.

Hostname Configuration

Edit your hostname with

```
vi /etc/hostname
```

or by pasting the following command to use the hostname router:

```
echo router >> /etc/hostname
```

It is not required to set the hostname.

Network Interface Configuration

> **Note**
>
> For a proper configuration, you will have two network interfaces for an internal and external zone (unless both internal and external zones reside on the same network interface, see [single interface configuration](#Single Interface Configuration)).

Multi-interface Configuration

We will assume eth0 is your external interface. Swap the instructions if eth0 is internal.

Open up your ifcfg-eth0 configuration:

```
vi /etc/sysconfig/network-scripts/ifcfg-eth0
```

Set the following lines to the values corresponding, or create the lines if they don't exist.

```
BOOTPROTO=static
ONBOOT=yes
IPADDR="${EXTERNAL_IP}"
NETMASK="${EXTERNAL_NETMASK}"
GATEWAY="${EXTERNAL_GATEWAY}"
DNS1="${EXTERNAL_DNS}"
ZONE=external
```

Reload the interface after saving the changes above.

```
ifdown eth0 && ifup eth0
```

OR

```
systemctl restart network
```

After doing this, you should be able to ping the upstream gateway (172.18.0.1).
Doing so will validate that external routing is properly configured.

Open up your ifcfg-eth1 configuration:

```
vi /etc/sysconfig/network-scripts/ifcfg-eth1
```

Set the following lines to the values corresponding, or create the lines if they don't exist. You DO NOT need to delete every other line in this file.

```
BOOTPROTO=static
ONBOOT=yes
IPADDR="${INTERNAL_IP}"
NETMASK="${INTERNAL_NETMASK}"
DNS1="${INTERNAL_DNS}"
ZONE=internal
```

Restart your network before continuing to configuration of the firewalld firewall with the following command:

```
systemctl restart network
```

Firewalld

Zones

An internal zone resides on your "internal" network interface, which would host the interface to connect your hosts to your router as a gateway.

An external zone resides on your "external" network, which would normally be mapped to your external IP address via DHCP, often assigned by an internet service provider. This can reside on the same interface as your internal zone depending on your configuration.

IP Forwarding

Modify

```
/etc/sysctl.d/ip_forward.conf
```

file with:

```
vi /etc/sysctl.d/ip_forward.conf
```

and add the following line to the file:

net.ipv4.ip_forward=1

Alternatively, you could paste this to your terminal:

```
echo net.ipv4.ip_forward=1 > /etc/sysctl.d/ip_forward.con
```

Reload IP Forwarding Configuration

Execute the following command to reload the ip_forward.conf configuration file.

```
sysctl -p /etc/sysctl.d/ip_forward.conf
```

Enable IP Masquerading

This will allow IP masquerading across the internal and external interfaces.

```
firewall-cmd --permanent --direct --passthrough ipv4 -t nat -I POSTROUTING -o
eth0 -j MASQUERADE -s ${INTERNAL_IP}/${NETMASK}
```

If you are unsure what the netmask CIDR is for your installation, you could use ${INTERNAL_IP}/24 by default.

Assign interface to external zone

For this tutorial, eth0 is our external interface. Depending on your setup, this could be swapped. Assign eth0 to our external interface with the following command:

```
firewall-cmd --change-interface=eth0 --zone=external --permanent
```

Set internal zone as default

Set the internal zone as the default zone for firewalld to perform routing with:

```
firewall-cmd --set-default-zone=internal
```

Reload firewalld so your changes take effect:

```
firewall-cmd --complete-reload
```

List Firewall Rules

You can list your firewall rules on your internal and external zones with the following commands:

```
firewall-cmd --list-all

firewall-cmd --list-all --zone=external

firewall-cmd --list-all --zone=internal
```

Port Forwarding

Some services may require a port forward on the router to properly score. Refer to the topology map to help determine which servers may require a port forward.

Example:

```
firewall-cmd --zone=external --add-forward-
port=port=80:proto=tcp:toport=80:toaddr=192.168.t.5
```

Configure an internal host

After all is said and done, it's not very useful to have your CentOS host configured as a router if you don't use it. Be sure you have a host connected on the same interface as the internal interface of your router.

Configure a static address on your machine using your router's internal IP address as your gateway; be sure your netmask and address are on the same subnet as your gateway address is on.

Validate Connectivity

External Interface

At this point, both your external and internal interfaces should be configured. As long as DNS is setup, you should be capable of pinging Google and getting a response similar to below:

```
PING google.com (172.217.3.110) 56(84) bytes of data.
64 bytes from lga34s18-in-f14.1e100.net (172.217.3.110): icmp_seq=1 ttl=52
time=53.9 ms
64 bytes from lga34s18-in-f14.1e100.net (172.217.3.110): icmp_seq=2 ttl=52
time=33.9 ms
64 bytes from lga34s18-in-f14.1e100.net (172.217.3.110): icmp_seq=3 ttl=52
time=37.1 ms
64 bytes from lga34s18-in-f14.1e100.net (172.217.3.110): icmp_seq=4 ttl=52
time=38.0 ms

--- google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 6ms
rtt min/avg/max/mdev = 33.920/40.725/53.864/7.739 ms
```

Internal Interface

You should also be able to ping your shell server from the internal network at this point so long as it is online.