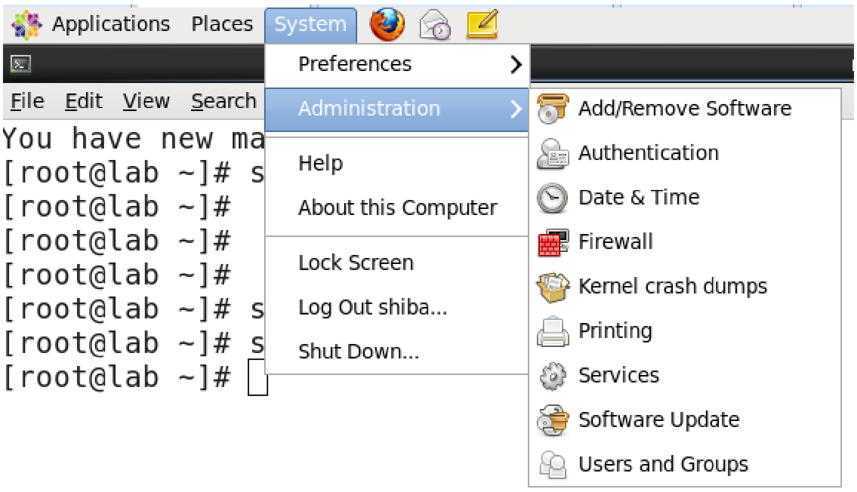
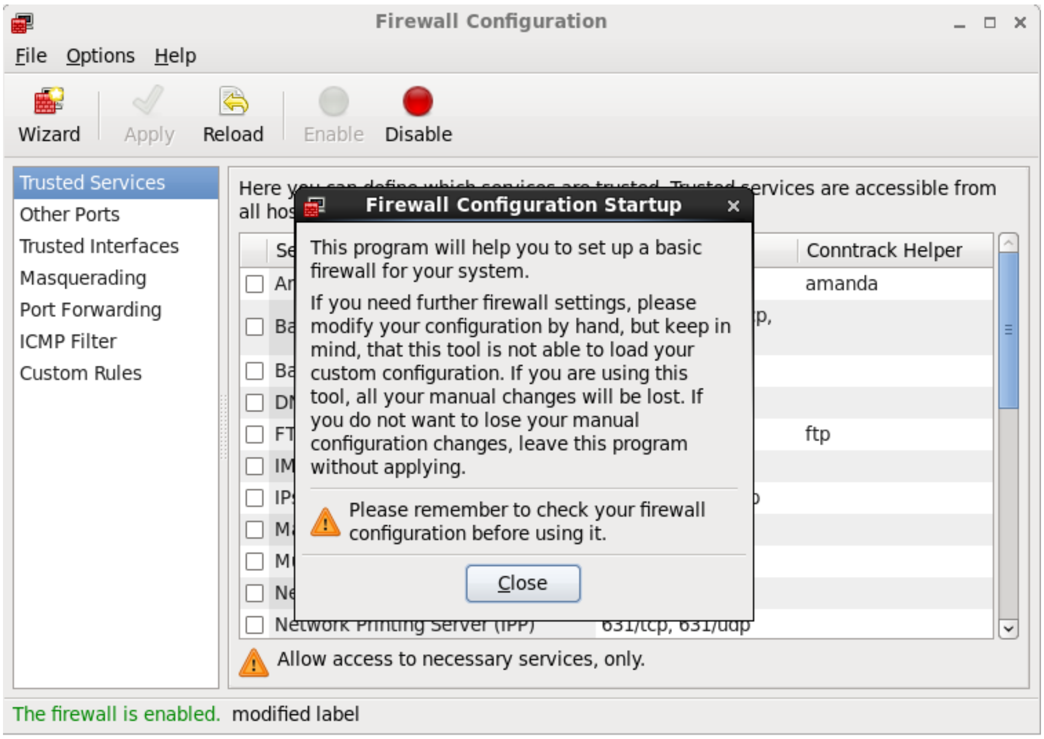
Configuring basic Firewall rules (iptables) from GUI

1. Select firewall from System -> Administration->Firewall menu.



```
You have new ma
[root@lab ~]# s
[root@lab ~]#
[root@lab ~]#
[root@lab ~]#
[root@lab ~]# s
[root@lab ~]# s
[root@lab ~]#
```

2. Click close to acknowledge that you are aware that only basic firewall configuration can be done with GUI interface and if you need additional configurations you should use iptables command from terminal.



Here y... ...ervices are accessible from all hos...

This program will help you to set up a basic firewall for your system.

If you need further firewall settings, please modify your configuration by hand, but keep in mind, that this tool is not able to load your custom configuration. If you are using this tool, all your manual changes will be lost. If you do not want to lose your manual configuration changes, leave this program without applying.

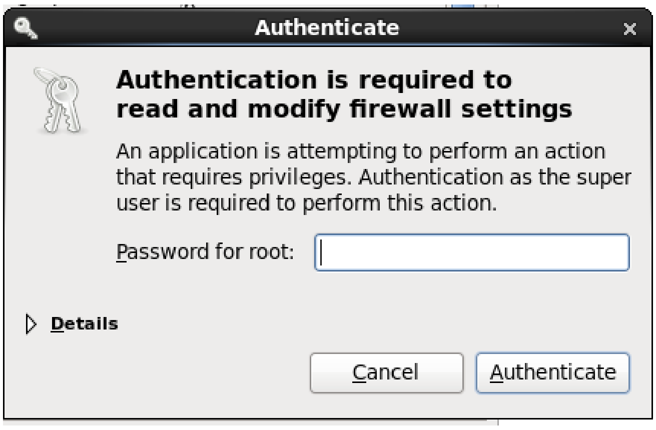
Please remember to check your firewall configuration before using it.

Network Printing Server (IPP) 631/tcp, 631/udp

Allow access to necessary services, only.

The firewall is enabled. modified label

3. If you are not logging GUI as root user, you will be asked to provide root's password for authentication. Give root's password and continue.



Authenticate

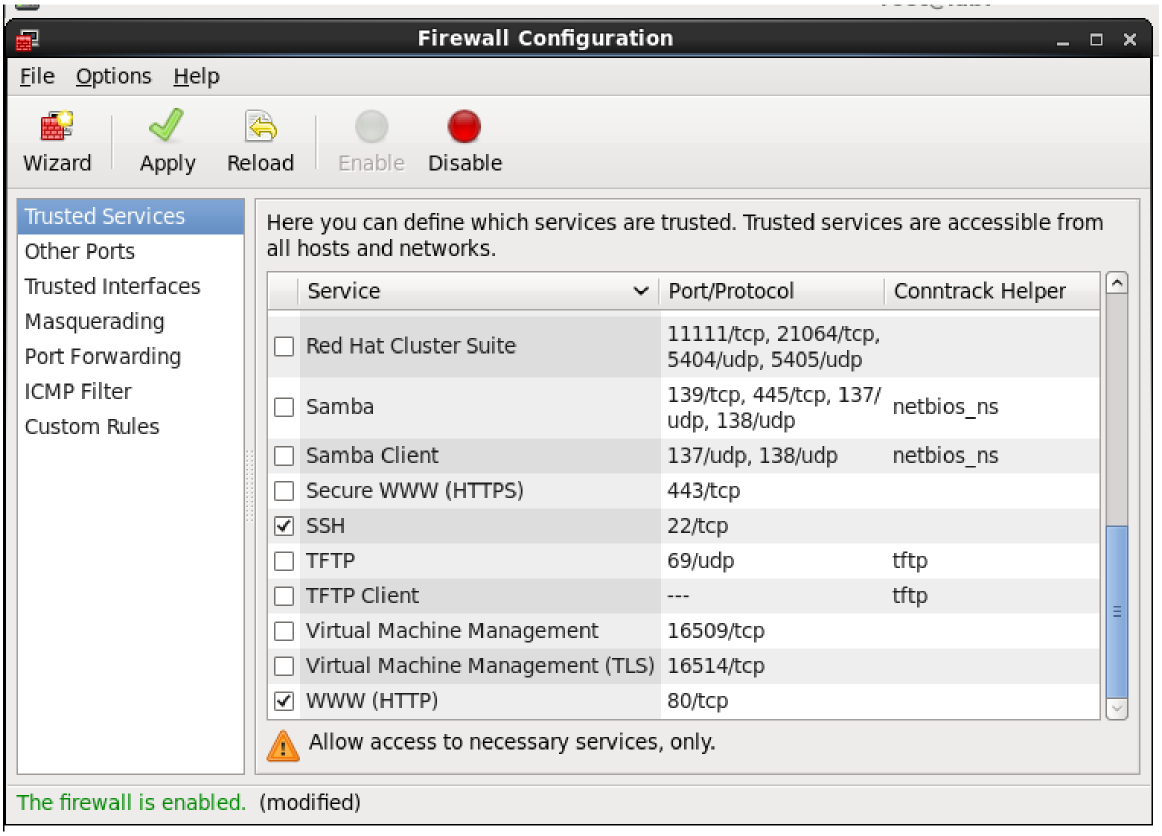
Authentication is required to read and modify firewall settings

An application is attempting to perform an action that requires privileges. Authentication as the super user is required to perform this action.

Password for root:

▷ Details

4. You are now in position to select any service in the list to allow or disallow through firewall. For instance in following diagram, I have selected WWW (HTTP) and clicked to Apply



Firewall Configuration

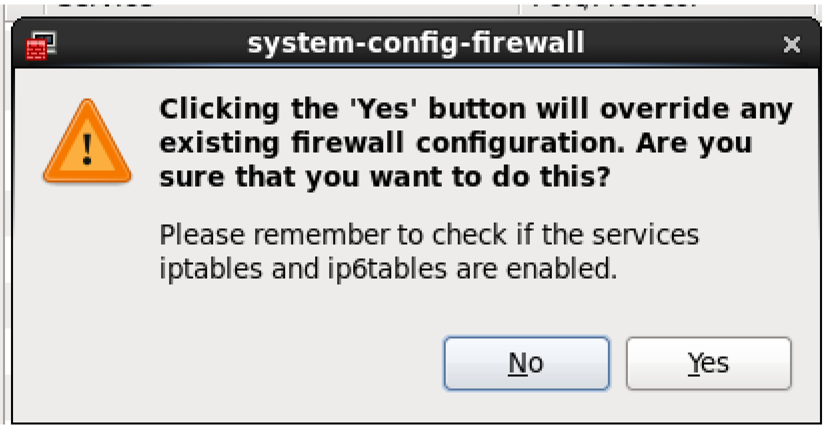
Here you can define which services are trusted. Trusted services are accessible from all hosts and networks.

	Service	Port/Protocol	Conntrack Helper
□	Red Hat Cluster Suite	11111/tcp, 21064/tcp, 5404/udp, 5405/udp	
□	Samba	139/tcp, 445/tcp, 137/udp, 138/udp	netbios_ns
□	Samba Client	137/udp, 138/udp	netbios_ns
□	Secure WWW (HTTPS)	443/tcp	
☑	SSH	22/tcp	
□	TFTP	69/udp	tftp
□	TFTP Client	---	tftp
□	Virtual Machine Management	16509/tcp	
□	Virtual Machine Management (TLS)	16514/tcp	
☑	WWW (HTTP)	80/tcp	

⚠ Allow access to necessary services, only.

The firewall is enabled. (modified)

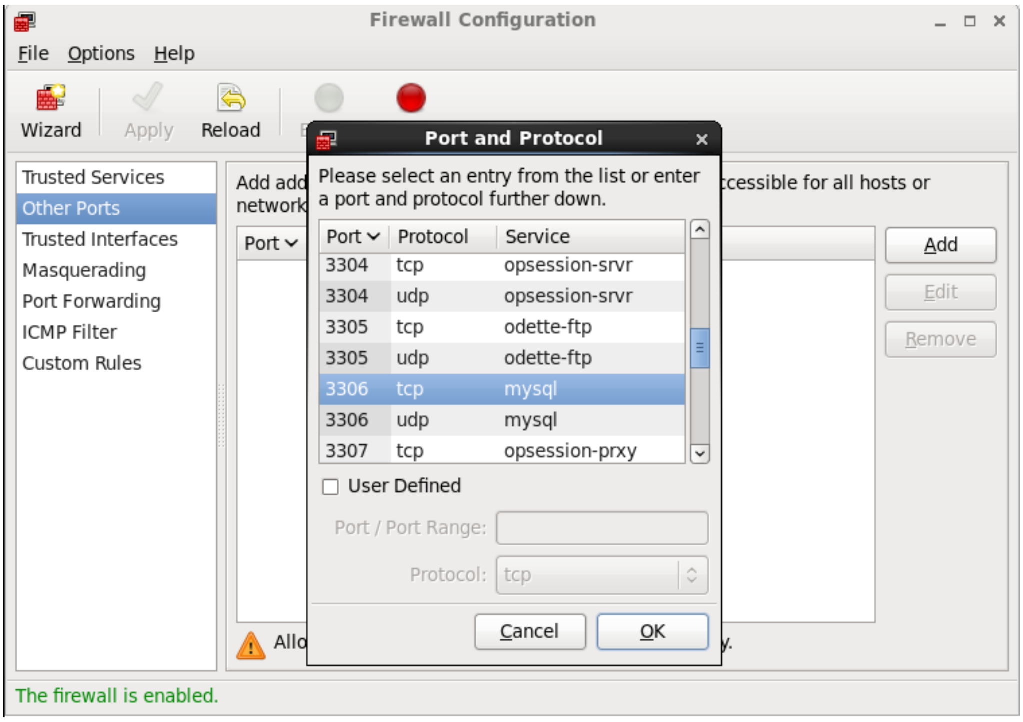
5. Once you clicked to Apply you will be prompt to dialog box for conformation to override existing rules. Click to yes.



Clicking the 'Yes' button will override any existing firewall configuration. Are you sure that you want to do this?

Please remember to check if the services iptables and ip6tables are enabled.

6. Similarly, you can repeat same process to allow in-bound traffic through firewall
7. To enable mysql access from remote computer click on “other ports” in Left menu and select 3306/tcp in list and click to ok



Please select an entry from the list or enter a port and protocol further down.

Port	Protocol	Service
3304	tcp	opsession-srvr
3304	udp	opsession-srvr
3305	tcp	odette-ftp
3305	udp	odette-ftp
3306	tcp	mysql
3306	udp	mysql
3307	tcp	opsession-prxy

The firewall is enabled.

8. More discussion on Firewall will be done in “Router Configuration” section of last chapter.

Note: The configuration is saved in the file */etc/sysconfig/system-config-firewall* when clicking **Apply** then file */etc/sysconfig/iptables* is overwritten.

Configuring basic Firewall rules (iptables)

To add httpd and mysqld service in trusted service or to allow income traffic for port 80 and 3306

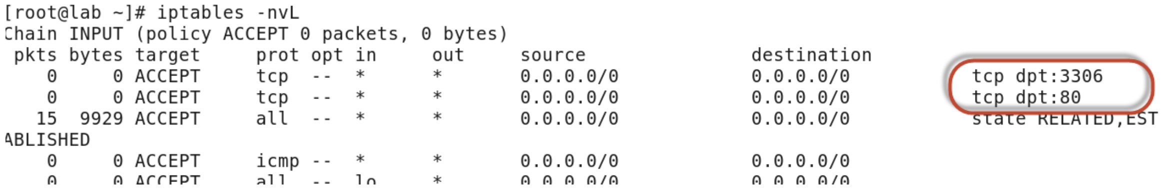
```
#Allowing income traffic of port 80 to the server

iptables -I INPUT -p tcp - -dport=80 -j ACCEPT

#Allowing income traffic of port 80 to the server

iptables -I INPUT -p tcp - -dport=3306 -j ACCEPT
```

# saving added rules to firewall into file /etc/sysconfig/iptables

service iptables save

# to verify if the rule is added or not use following commands, use man to know about the #options n, v and L in detail

iptables -nvL



```
[root@lab ~]# iptables -nvL
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:3306
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:80
   15  9929 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           state RELATED,EST
ABLISHED
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            0.0.0.0/0
    0     0 ACCEPT     all  --  lo     *       0.0.0.0/0            0.0.0.0/0
```

Note: I have covered only basic rules to allow traffic to trusted services, if you want to know more about iptables go through different books of Linux firewall or following reference links. I will cover some more detail on iptables policies, port forwarding and masqueriding in "Router configuration" section in last chapter.

Further study:

http://www.howtogeek.com/177621/the-beginners-guide-to-iptables-the-linux-firewall/

http://fedoraproject.org/wiki/How_to_edit_iptables_rules

http://linuxtips-nitin.blogspot.com/2009/03/linux-iptables-configuration-step-by.html