

Table Of Contents

Table Of Contents	1
-------------------------	---

[Home](#) > [Faq](#) > [CentOS](#)

How to: Allow telnet and ssh through iptables under Linux

Posted by [Vivek Gite](#) <vivek@nixcraft.com>

Q. I run both RHEL / CentOS Linux server and by default firewall blocked out everything including telnet / ssh access. How do I allow telnet - port 23 and ssh port 22 through Linux iptables firewall ?

A. By default firewall rules stored at /etc/sysconfig/iptables location / file under CentOS / RHEL. All you have to do is modify this file to add rules to open port 22 or 23.

Login as the root user.

Open /etc/sysconfig/iptables file, enter:

```
# vi /etc/sysconfig/iptables
```

Find line that read as follows:

```
COMMIT
```

To open port 22 (ssh), enter (before COMMIT line):

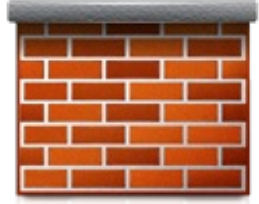
```
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
```

To open port 23 (telnet), enter (before COMMIT line):

```
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 23 -j ACCEPT
```

Save and close the file. Restart the firewall:

```
# /etc/init.d/iptables restart
```



[1]

4000+ howtos and counting! Want to read more Linux / UNIX howtos, tips and tricks? Subscribe to our [daily email](#) newsletter or [weekly newsletter](#) to make sure you don't miss a single tip/tricks. Alternatively, subscribe via [RSS/XML](#) feed.

Article printed from Frequently Asked Questions About Linux / UNIX: <http://www.cyberciti.biz/faq/>

URL to article: <http://www.cyberciti.biz/faq/linux-open-iptables-firewall-port-22-23/>

URLs in this post:

[1] Image: <http://www.cyberciti.biz/faq/faq/category/iptables/>