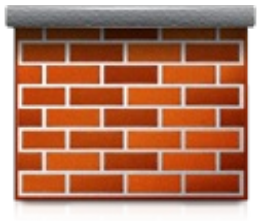
Table Of Contents

nixCraft: Linux Tips, Hacks, Tutorials, And Ideas In Blog Format
http://www.cyberciti.biz/

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 thought 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. [1]

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
```