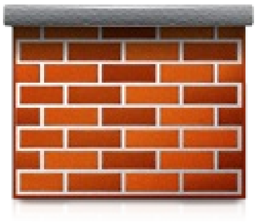
Table Of Contents

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

Home > Faq > CentOS

Linux Iptables Allow NFS Clients to Access the NFS Server

Posted by Vivek Gite <vivek@nixcraft.com>



[1]

The portmapper assigns each NFS service to a port dynamically at service startup time. How do I allow legitimate NFS clients to access the NFS server using RHEL / Fedora / CentOS Linux 5.x iptables firewall?

You need to open the following ports:
a] **TCP/UDP 111** - RPC 4.0 portmapper

b] **TCP/UDP 2049** - NFSD (nfs server)

c] **Portmap static ports** - Various TCP/UDP ports defined in /etc/sysconfig/nfs file.

Configure NFS Services to Use Fixed Ports

However, NFS and portmap are pretty complex protocols. Firewalling should be done at each host and at the border firewalls to protect the NFS daemons from remote
access, since NFS servers should never be accessible from outside the organization. However, by default, the portmapper assigns each NFS service to a port dynamically at service startup time. Dynamic ports cannot be protected by port filtering firewalls such as iptables. First, you need to configure NFS services to use fixed ports. Open /etc/sysconfig/nfs, enter:

```
# vi /etc/sysconfig/nfs
```

Modify config directive as follows to set TCP/UDP unused ports:

```
# TCP port rpc.lockd should listen on.
LOCKD_TCPPORT=lockd-port-number
# UDP port rpc.lockd should listen on.
LOCKD_UDPPORT=lockd-port-number
# Port rpc.mountd should listen on.
MOUNTD_PORT=mountd-port-number
# Port rquotad should listen on.
RQUOTAD_PORT=rquotad-port-number
# Port rpc.statd should listen on.
STATD_PORT=statd-port-number
# Outgoing port statd should used. The default is port is random
STATD_OUTGOING_PORT=statd-outgoing-port-numbe
```

Here is sample listing from one of my production NFS server:

```
LOCKD_TCPPORT=32803
LOCKD_UDPPORT=32769
MOUNTD_PORT=892
RQUOTAD_PORT=875
STATD_PORT=662
STATD_OUTGOING_PORT=2020
```

Save and close the files. Restart NFS and portmap [2] services:

```
# service portmap restart
# service nfs restart
# service rpcsvcgssd restart
```

Update /etc/sysconfig/iptables files

Open /etc/sysconfig/iptables, enter:

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

Add the following lines, ensuring that they appear before the final LOG and DROP lines for the RH-Firewall-1-INPUT chain:

```
-A RH-Firewall-1-INPUT -s 192.168.1.0/24 -m state --state NEW -p udp --dport 111 -j ACCEPT
-A RH-Firewall-1-INPUT -s 192.168.1.0/24 -m state --state NEW -p tcp --dport 111 -j ACCEPT
-A RH-Firewall-1-INPUT -s 192.168.1.0/24 -m state --state NEW -p tcp --dport 2049 -j ACCEPT
-A RH-Firewall-1-INPUT -s 192.168.1.0/24  -m state --state NEW -p tcp --dport 32803 -j ACCE
-A RH-Firewall-1-INPUT -s 192.168.1.0/24  -m state --state NEW -p udp --dport 32769 -j ACCE
-A RH-Firewall-1-INPUT -s 192.168.1.0/24  -m state --state NEW -p tcp --dport 892 -j ACCEPT
-A RH-Firewall-1-INPUT -s 192.168.1.0/24  -m state --state NEW -p udp --dport 892 -j ACCEPT
-A RH-Firewall-1-INPUT -s 192.168.1.0/24  -m state --state NEW -p tcp --dport 875 -j ACCEPT
-A RH-Firewall-1-INPUT -s 192.168.1.0/24  -m state --state NEW -p udp --dport 875 -j ACCEPT
-A RH-Firewall-1-INPUT -s 192.168.1.0/24  -m state --state NEW -p tcp --dport 662 -j ACCEPT
-A RH-Firewall-1-INPUT -s 192.168.1.0/24 -m state --state NEW -p udp --dport 662 -j ACCEP
```

Save and close the file. Replace 192.168.1.0/24 with your actual LAN subnet /mask combo. You need to use static port values defined by /etc/sysconfig/nfs config file. Restart iptables service:

```
# service iptables restart
```

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

URL to article: **http://www.cyberciti.biz/faq/centos-fedora-rhel-iptables-open-nfs-server-ports/**

URLs in this post:

[1] Image: **http://www.cyberciti.biz/faq/category/iptables/**
[2] NFS and portmap: **http://www.cyberciti.biz/faq/how-do-i-start-and-stop-nfs-service/**