# Table Of Contents

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



# Howto Secure portmap service using iptables and TCP Wrappers under Linux

Posted by Vivek Gite <vivek@nixcraft.com>

Q. How do I secure the portmap service? I am using Debian Linux.

A. According to wikipedia [1], "*Portmap is server software running under Unix-like systems that converts RPC program numbers into DARPA protocol port numbers. Its design objective was to minimize the number of ports in use, but this never happened as it never had wide adoption. It must be running in order to make RPC calls.*"

When an RPC server is started, it will tell portmap what port number it is listening to, and what RPC program numbers it is prepared to serve. When a client wishes to make an RPC call to a given program number, it will first ontact portmap on the server machine to determine the port number where RPC packets should be sent.

It is **extensively used** by NIS, NFS, and FAM. It is used to **assign a dynamic port** to NIS and NFS.

You can protect portmap with:
=> TCP Wrappers

=> Iptables

## TCP Wrappers

If you're going to protect the portmapper use the name "portmap" for the daemon name. Remember that you can only use the keyword "ALL" and IP addresses (NOT host or domain names) for the portmapper, as well as for rpc.mountd (the NFS mount daemon).
Open /etc/hosts.allow file:

```
# vi /etc/hosts.allow
```

Sample entires for portmap server to allow access from 192.168.1.0/24 only.

```
sshd : ALL
portmap : 192.168.1.0/24
```

Save and close the file.

## IPTables portmap rules

Portmap listens on port 111. Add following rules to your iptables:

Drop UPD port 111 packets if they are not from 192.168.1.0/24

```
iptables -A INPUT -p udp -s! 192.168.1.0/24 --dport 111 -j DROP
```

Drop TCP port 111 packets if they are not from 192.168.1.0/24 and localhost (127.0.0.1)

```
iptables -A INPUT -p tcp -s! 192.168.1.0/24 --dport 111 -j DROP
iptables -A INPUT -p tcp -s 127.0.0.1 --dport 111 -j ACCEPT
```

For more information refer to following man pages:

```
man iptables
man tcpd
man 5 hosts_access
man portmap
```

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-secure-portmap-with-iptables-tcp-wrappers/**

URLs in this post:

[1] wikipedia: **http://en.wikipedia.org/wiki/Portmap**

---