

Re: SCO 5.0.7 AS ROUTER

Source: <http://unix.derkeiler.com/Newsgroups/comp.unix.sco.misc/2005-05/0163.html>

From: Tom Parsons (*sconews_at_tegan.com*)

Date: 05/23/05

Date: 23 May 2005 17:36:18 -0400

Brian K. White enscribed:

```
|
| ----- Original Message -----
| From: "Jean-Pierre Radley" <jpr@jpr.com>
| Newsgroups: comp.unix.sco.misc
| To: <distro@jpr.com>
| Sent: Sunday, May 22, 2005 12:33 PM
| Subject: Re: SCO 5.0.7 AS ROUTER
|
|
| > Mainak Yajnik typed (on Sun, May 22, 2005 at 09:04:41AM -0700):
| > | I refered the document mentioned above in the message,
| > |
| > | Issued the command after login as root
| > |
| > | ipnat -FC -f - <<EOF
| > | >map net0 203.112.130.18/24 - 192.168.0.227/24
| > | >EOF
| > |
| > | It still does not passon the packets from 192,168.0.227 network to the
| > | internet 203.112.130.18 is the Public IP
| > |
| > | I assume that net0 is for the outside NIC, not the inside 192.168 NIC.
| > | If not, then you want the remapping to be on net1.
| > |
| > | Anyhow, you have it wrong. You want to map anything on 192.168.0 (a /24
| > | network) to the single public address at 203.112.130.18. And you need
| > | '->', not '-', in the map command.
| > |
| > | Put this into /etc/ipnat.rules:
| > |
| > | map net0 198.207.0.0/24 -> 203.112.130.18/32
| > |
| > | and run
| > | /etc/ipnat -CF -f /etc/ipnat.rules
| > |
| > | You should put that last command into /etc/rc.d/7/* so that it runs when
| > | you reboot,
```

|
| /etc/init.d/ipfnat already exists in the base system and it looks for
| /etc/ipnat.conf and /etc/ipf.conf
| put nat rules like above in /etc/ipnat.conf
| put firewall rules in /etc/ipf.conf
| you can run /etc/init.d/ipfnat stop/start whenever you want and symlink it
| to /etc/rc2.d/S99ipfnat so it runs at boot.

Really, really, really bad mistake.

That 'broken' script also starts ipf. Ipf should always be started before networking is started, so the latest it should run would be /etc/rc2.d/S84ipf.

This command in the distribution startup script is a security hole:

```
ipf -Fa -f /etc/ipf.conf
```

As long as you only run it at startup AND before tcp starts, no problem but if you run it after startup, there is a momentary opening in the firewall between erasing the old entries and loading the new entries and of course, if it should fail for some reason, the firewall is disabled.

Much better to run:

```
cat /etc/ipf.rules| ipf -If - && ipf -s -IF a
```

This loads the new rules into the inactive table, then swaps then with the active set only if the first command succeeds.

--

=====