

## OT: iptables rules request

**Source:** <http://linux.derkeiler.com/Mailing-Lists/Fedora/2005-05/4426.html>

---

**From:** James Pifer ([jep\\_at\\_obrien-pifer.com](mailto:jep_at_obrien-pifer.com))

**Date:** 05/31/05

To: Fedora <[fedora-list@redhat.com](mailto:fedora-list@redhat.com)>  
Date: Tue, 31 May 2005 11:04:29 -0400

I'm looking for some help with iptables. Anyone good in iptables willing to assist with (ie write) a few rules?

I have a box running iptables and there are three networks going through it.

eth0 is the local network 192.168.192.0  
eth1 is the internet  
ipsec0 is a vpn 172.16.0.0

Everything is good except I'd like to limit what machines on my 192.168.192 network can communicate over the ipsec0 connection. Here's what I'd like to accomplish:

- 1) Allow 192.168.192.2 to only use port 53 (UDP) through ipsec0
- 2) Allow 192.168.192.100 full access through ipsec0
- 3) Allow 192.168.192.10-192.168.192.25 full access through ipsec0
- 4) Disallow anything else through ipsec0

If I have this much, I figure I could use them as a template to do more. I've been digging through tutorials and googling for iptables stuff. Didn't find a lot dealing with three seperate NICs like this. I can kind of see what it might look like, but I really don't want to spend the whole day by trial and error getting this to work.

Anyone willing to assist (give) me rules that would do this?

Any help is appreciated.

James

--

fedora-list mailing list  
[fedora-list@redhat.com](mailto:fedora-list@redhat.com)  
To unsubscribe: <http://www.redhat.com/mailman/listinfo/fedora-list>