

How do I snoop unauthorised traffic

Source: <http://linux.derkeiler.com/Newsgroups/comp.os.linux.networking/2006-09/msg00180.html>

- *From:* Peter Lowrie <peterlowrie@xxxxxxxxxxxxxxxxx>
 - *Date:* Tue, 12 Sep 2006 00:46:53 +1200
-

One of the Windows 2000 boxes is sending data out of the network to some host on the internet. My gateway is Mandrake Linux 8.2 running straight iptables. I've tried tcpdump against the internet facing NIC but the data are inconclusive.

How do I determine what traffic is leaving the network and determine what host it is being sent to, then what string do I use in the /etc/sysconfig/iptables file to block it?

Thanks
Peter

.