

## Re: adsl router security

**Source:** <http://www.derkeiler.com/Newsgroups/comp.os.linux.security/2003-12/0247.html>

---

**From:** Bill Unruh ([unruh\\_at\\_string.physics.ubc.ca](mailto:unruh_at_string.physics.ubc.ca))

**Date:** 12/14/03

Date: Sun, 14 Dec 2003 10:25:36 +0000 (UTC)

]>I have an adsl 4 port router/modem, badged as 'spark' but with a conexant  
]>chipset. I have configured it to connect my local machines to the NAT, and  
]>used the virtual server feature to route packets on ports 21 and 80 to the  
]>FTP and http ports (proftpd & apache) of my server machine, which is on  
]>the same local network as my main machine. The server machine is also  
]>running ssh and mysqld but no other network services. The main machine is  
]>running apache, mysqld, qmail, portmap, gdomap, inetd, lpd, tcpserver,  
]>xfs-xtt, gnustep\_sndd and gdm.

]>

]>What I would like to know is whether the firewall on the router is likely  
]>to be enough to protect me from external attacks? Obviously it makes sense

It will be a line of defense. To make it the only line of defense would probably not be a great idea, but as a line amongst others, it should be fine. You should find out, if you can if the router is programable from its outbound connection (ie does the router allow anyone at all to get into its admin functions from the outbound port. It shouldn't. If it does, that is a weakness)

Remember all a firewall does is to prevent certain packets getting through if they are not addressed to the selected ports. You seem to want a huge number of ports to be open. that means that the protection is minimal of any firewall. Ie, what ports is the firewall on the router blocking?

]>to configure the local machines to be as secure as possible also, but are  
]>the firewalls on these routers good enough to rely on as a first line of  
]>defence, or should I put some more firewalling in behind the router. E.g.  
]>I could reconfigure the network so that the main machine can reach the net  
]>only through the server machine, and run a good linux firewall on that, or  
]>else get hold of another old pentium, put it in a cupboard somewhere, and  
]>use it just as a firewall for my whole network.

]>

]>I'm only using the machine for web browsing, email, newsgroups, and a bit  
]>of web design and programming, so security isn't crucially important, but  
]>I would like to at least take sensible precautions.