

## Re: Linksys WRT54G and Firewall software

---

*Source:* <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2007-03/msg00366.html>

---

- *From:* "Mr. Arnold" <"Mr. Arnold"@Arnold.COM>
  - *Date:* Mon, 26 Mar 2007 02:14:57 GMT
- 

Gerald Vogt wrote:

Leythos wrote:

3) The windows non-firewall included in XP SP2 will be more than enough, but, if you take your laptop to other networks (school, work, friends) it won't be enough in most cases.

That is not conclusive: The NAT does block (most) incoming connections. The XP SP2 firewall does block all (most) incoming connections when configured with no exceptions.

It blocks intrusions, but what holes does it have that have not yet been exposed? What about the next one that's found and exposes the system?

Vulnerabilities which have not yet been exposed are always a problem. But you have the same problem with a NAT router, too. For the XP SP2 firewall is has been very much tested. NAT routers don't undergo that thorough tests simply because they are not used so much out there.

I would say that routers are used more and more by those who are informed. Routers do come with SPI (Statefull Packet Inspection), look it up if you don't know what it means.

Plus: it is in the nature of NAT that there is a lot of guessing involved which ports to open and which not. The router must let response packets in and must figure out where to send it. Thus, if you use a packet sniffer or use some logging functions on the computer you'll see that some unsolicited packets occassionally get through.

Re: Linksys WRT54G and Firewall software

Not with any router that's running SPI.

Where is the difference which explains why something else then the XP SP2 FW is needed elsewhere?

The NAT router is the better first line of defense when it can be used,

The XP SP2 FW with no exceptions on a computer directly connected to the internet is protecting the computer better than a NAT router. NAT does not provide the protection like a properly setup packet filter.

Do you know what SPI is?

but, as the OP mentions wireless, well, you can't NAT a wireless connection – what I mean is that the wireless connection is from the router to the laptop, there is no intermediate NAT between the wireless and the laptop – so, anything that makes it to the wireless also makes it to the laptop unless it's got some form of localized firewall.

That does not explain why the computer would need another (different) firewall from the XP SP2 FW when it is connected to other networks.

You have not explained why the XP FW it's better. XP's FW may be on par with a NAT router that's running SPI.

4) If you use your laptop on OTHER networks you really need to learn how to check the Windows TCP/IP Settings, disable File/Printer sharing when you are not home, and how to adjust/check the Windows XP SP2 non–firewall settings for "Exceptions".

## Re: Linksys WRT54G and Firewall software

Again contradictory to 3): if you think you need something else than the XP SP2 firewall in other networks and you are running a other brand "non-firewall" software then the recommendation should be to check that the XP SP2 firewall is turned off and the 3rd party "non-firewall" is on. Two or more firewalls running on a computer result on average in less security then a single one as it is unpredicted what actually is blocked and what not and by which firewall which will jeopardize the consistency of and state table in any firewall (as they are generally stateful).

I never mentioned another firewall application, not a single one, not even suggesting it. Stop playing the old/tired mantra.

Well you wrote: "The windows non-firewall included in XP SP2 will be more than enough, but, if you take your laptop to other networks school, work, friends) it won't be enough in most cases.". If it is not a 3rd party firmware then what else do you need? You don't explain it. I have guess you have thought of a 3rd party firmware. If it is not, then you really have to explain what would fill the "not enough" if the computer is in other networks.

You can't read and understand English.

5) More important than a firewall, when behind a NAT router, is the Antivirus software and your security methods – like not running as an Administrator (best to run as a limited user), installing Fire Fox, not using Outlook Express or Outlook if you use POP3 for email....

Most important to keep your system up-to-date and reduce the number of software on your computer. The less software you are running the less is vulnerable. The less software the less you have to check for updates manually if it does not come with automatic updates. Subscribe to some good security notification lists like the one from Microsoft or US-Cert. Then you get timely notification of updates and you can update very quickly.

If you do all this you are very likely that your AntiVirus will

Re: Linksys WRT54G and Firewall software

never ever report anything relevant and thus will prove itself superfluous.

So you mean that if you access email, through POP3, that you don't need antivirus? So, you mean that if you download via FTP or other, since the net has more than just MS and Cert, that you don't really need AV?

I access my e-mails through pop3 and imap. I don't need antivirus. Why should I need antivirus? For what? The antivirus usually does not show any useful messages. All the antivirus potentially did was damaging my mail folders when the mail program downloaded an old blaster from my pop3 box and annoyed me with some 20 virus access warnings (which I had to allow each time) until I was able to delete the virus e-mail from my Inbox and emptied the trash. The computer was at no time at any danger still the antivirus will give you a hard time to do what you are supposed to do with an virus e-mail: DELETE.

Well, the AV that I use has IMON (Internet Monitor) that will detect anomalies coming in the TCP connection, stop it and allow me to terminate the connection. This allows be to use an email proxy client application to go to the ISP's email server and delete the suspicious email. The email never reaches my machines.

And what should I donwload via FTP for which I need an antivirus? Can you be more specific?

An infected or dubious file can be downloaded from a FTP site. Do you think it cannot happen?

Come one, AV is mandatory, even as a limited user, for anyone running an OS that can be exploited by malware.

No. I don't have AV nor FW. I run as limited user. I don't know why it should be mandatory. As there is no 100% security anything can potentially be exploited by malware. But the best protection against malware is still me. As I am better than some AV which well slows down my computer it is a easy choice for me.

That's you. You make your own bed and you lay in it. One doesn't rely on detection software like a crutch, but they don't hurt in the prevention.

For a machine that has a direct connection to the modem and to the Internet, a user would be some kind of fool not to run what an AV and some kind of PFW/personal packet filter or XP's FW/personal packet filter, if

Re: Linksys WRT54G and Firewall software

using the XP O/S or some other MS NT based O/S.