

Regarding Personal Computer Software Firewalls

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2005-11/0443.html>

From: Kyle Stedman (kyle_st_at_yahoo.com)

Date: 11/20/05

Date: Sun, 20 Nov 2005 19:22:01 GMT

Below is pasted an interesting article. Comments?

"Personal Firewalls" are mostly snake-oil

A 'personal firewall' isn't a firewall. A firewall is a dedicated box with (usually) two or three ethernet ports running no services other than a firewall. My preferred configuration is an x86 box with a couple of tulip cards running FreeBSD or OpenBSD and ipf, though you can do OK with Linux and iptables too. You can run either on a \$100 obsolete PC. (*BSD is better, but Linux is easier for a new user to configure).

Even the little hardware NAT boxes that you can get for sharing a DSL connection or cable modem are way better than any 'software firewall' (The NetGear RT311 and RT314 are extremely sophisticated and flexible NATs and start at less than \$100 – they do full NATing, allow port forwarding and filtering to a protected network (NetGear Firewalls and NATs).

So... what does a 'personal firewall' actually do? Well, effectively it listens on all the ports on your system. This provides no real additional security over turning off the services that you don't use.

I'll repeat that – it provides no real additional security over turning off the services that you don't use. (Maybe it'll block trojans from phoning home, but A) if you've run a trojan your system is completely compromised and B) <http://cyberpunks.org/display/356/article/>).

What it does do is break standard network applications (such as traceroute) and, more importantly, if badly written it will claim normal background network traffic is some sort of attack, alarming the user for no good reason. I've never heard of a 'personal firewall' that isn't badly written in this way. That doesn't mean one doesn't exist.

Why do the authors do this? Two reasons, as far as I've been able to gather.

The first is that most of the people writing these applications know next to nothing about IP networking. They may be pretty good windows

comp.security.firewalls: Regarding Personal Computer Software Firewalls

developers, but they have no idea what normal network traffic looks like. That should make you nervous about their ability to block any real malicious intent.

The second is more insidious... Why is an end user going to buy / register / upgrade their 'personal firewall'? They're not going to do so if they don't perceive any benefit from it. If it were a properly written application that just sat there, doing its job quietly in the background, users would forget it was there. But if it pops up warnings about 'attacks' all the time then it's clearly Doing Something. Most of those warnings are entirely frivolous – normal network traffic. And the remaining few... well... if the 'personal firewall' has protected your system from the supposed 'attack'... why do you care about it? You're safe from that supposed 'attack', right? So why pop up warnings and alerts? To make you feel you're getting a service from this program and so you'll pay for updates or 'Pro' versions.

The bottom line is this... If you care about your home network security a lot, and you're interested in it, spend the time to learn about networking and build yourself a standalone firewall.

If you don't want to spend that amount of energy on it, buy a standalone dedicated NAT or NAT+firewall box. I like the NetGear RT-311 and its siblings, but there're a bunch of others out there too. It'll sit there, do its job and never bother you again.

If you want to play with a piece of windows software that makes you click all over the place, there's always minesweeper.

If you'll feel safer sleeping at night knowing there's a 'personal firewall' running on your system, then install one. As long as you pay no attention to the "hack attacks" it reports it's better than nothing. A free one, ideally, as few of them are worth paying for. Turn off all the alerts and logging – you'll just waste your time (and, more importantly to me, my time and the time of other network administrators your complaints go to) increase your blood pressure and provide no benefit to you. If you really want to leave them turned on and see where traffic is coming from, feel free, but remember that most of the traffic you see is harmless, and that even if it isn't harmless it can't affect your system (if it could, it wouldn't be logged). Oh, and try not to waste admins time with frivolous complaints.

"But, but, but reporting these alerts to network administrators will help them catch crackers!"

Uhm, no. I know a whole bunch of network security and abuse staff. The response to any complaint with ZoneAlarm, BlackIce etc logfiles in it is to close the ticket, usually with an annotation like 'GWF' (Goober with Firewall). 99% of those reports are frivolous, about normal network traffic. In the remainder of cases there's nowhere near enough data in the logfiles to provide any idea of why the end user is upset. If you

comp.security.firewalls: Regarding Personal Computer Software Firewalls

send frivolous complaints that just wastes the time of the staff receiving them and prevents them from handling real security issues. How do you tell if a complaint is frivolous? If the sender doesn't understand basic networking, it's almost certainly frivolous. If the sender is complaining based on 'personal firewall' logs, it's definitely frivolous.

The abuse desk staff I talk with hate users of 'personal firewalls' more than they hate spammers. That should tell you something about how useful your complaints will be.

"You're just a unix bigot and don't like Windows applications!"

I don't like Windows applications for networking, no, as Windows isn't very good at it in general (with a few exceptions – some of the kernel level networking code in NT4 and NT5 is extremely sophisticated). As for being a unix bigot... I'm a Microsoft Independent Software Vendor, subscribe to Microsoft Developers Network and in my spare time produce Windows Network Applications.

From: <http://www.samspace.org/d/firewalls.html>