

Re: Alternatives to using a Personal Firewall

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2006-06/msg00674.html>

- *From:* B. Nice <b_nice@xxxxxxxxxxx>
 - *Date:* Thu, 29 Jun 2006 06:25:54 GMT
-

On Wed, 28 Jun 2006 19:26:47 -0700, zzy <anon@xxxxxxxxxxx> wrote:

The point I keep getting stuck at is the part about "disabling unnecessary services". On my machine right now, there are 109 services listed, of which 61 are running. In the past I've tried disabling various ones, and often discovered some time later that some application or other has stopped working properly. I never get an error message that the reason is due to a stopped service, so end up burning a lot of time discovering that, then figuring out which one(s) I have to restart. I see that I could easily spend a very great deal of time doing this "disabling unnecessary services" bit which the experts toss off as a trivial matter.

I get Your point. My idea was definately not to go through all the services running, unless You are very sensitive to Your CPU usage. For a novice that will undoubtly lead to trouble with applications that suddenly won't work. Don't do that!

You just need to disable those services that are in a network listening state and that You don't need. I would like to be able to post links to good step-by-step guides but haven't done much googling for english ones. I have some very good guides that even a novice can use to harden his/her machine in less than half an hour. But unfortunately they are in my native language.

My main machine is behind a hardware router and is on all day every day. So far, nothing malicious has gotten in. So I'm satisfied with the security the router provides. Like some other folks who've commented here, I like to know what's "phoning home" and often prohibit it -- Windows Media Player, Windows Genuine Advantage Notification (every time I boot), PGP Tray, Real Player, and on and on. Windows (the MS DTC Console) even tries to call home every time I compile a VB program. This is maybe not a security issue, but neither is closing my window shades at night when everybody walking by can look in -- and I do that, too. A number of desktop firewalls give me the ability to stop at least some of this "phoning home".

Re: Alternatives to using a Personal Firewall

For me that doesn't make sense. If I don't trust the program vendor to be serious about my privacy I will not allow it on my machine. As PFW's are concerned, I personally wouldn't install a big chunk of code just to be able to control "home phoning".

However, if it makes sense to You, that's fine. We are all different. As long as people don't put it into a security context claiming that they will prevent malware from doing nasty stuff it's fine with me. When malware is already run, damage is done. No matter what people claim. The hard but real trick is to prevent it in the first place.

My main concern is my laptop machine, which I take when I travel. It has ample opportunity to pick up malware from the various wired and wireless networks I connect to when on the road. Without the benefit of a hardware router, it needs some kind of protection.

If running TCP/IP on Your LAN, yes. In those cases I would recommend a simple packet filter like the windows firewall or as an alternative for non-XP's like W2K the CHX-I packet filter with "workstation" setup or, if You are a little techy, You could even configure the build-in IP filter.

The reason I recommend those is, that they do what they are supposed to without asking silly questions.

Like my other machines, I keep it backed up. But it would be a genuine nuisance if it picked up some malware then distributed it to the other machines on my home LAN when I brought it back and hooked it in. So a layer of protection beyond the router for all the machines on my LAN seems prudent. My laptop, like my home machine, isn't just an email-and-surfing toy, but one with a large number of applications and the need to be able to ftp files to and from my web site, download software and patches, and the like.

Very good point. If You have it connected to Your LAN at home and occasionally takes it outside there are special issues not covered by my guide. My guide, as posted, was targeted primarily at stand-alone machines with an internet-connection – which unfortunately wasn't too obvious. I am currently working on putting up a web-site with ground rules (or traffic rules) that even a novice should be able to follow. I am struggling to make it very precise. But since English isn't my native language it takes some time.

So, is there any methodical way to close ports and disable unneeded services other than try this and that and see what it breaks, and "Search the net and seek help in relevant forums"?

Re: Alternatives to using a Personal Firewall

Yes. I will see if I can google You some good ones.

When faced with the task of doing that for 61 running services and another bunch of automatic ones which can be started without my explicitly starting them, I'd just about as soon take my chances with a personal firewall.

Very understandable.

.