

Re: Trying to Figure out What's OK and What to Block

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2006-03/msg00306.html>

- *From:* Kerodo <loopback@xxxxxxxxxxxxxx>
 - *Date:* Fri, 10 Mar 2006 17:02:44 -0800
-

In article <ce2412pq51rdsbnm2ns8f8c4rpp5j1ns3@xxxxxxx>, fishlips@xxxxxxxxxxxxxxxxxxxxxxxxxxxx says...

On Fri, 10 Mar 2006 14:50:54 -0800, Kerodo <loopback@xxxxxxxxxxxxxx> wrote:

In article <4uo312t5qp4me94i3rg9bgc9v91781qtl4@xxxxxxx>, fishlips@xxxxxxxxxxxxxxxxxxxxxxxxxxxx says...

I have a Win Xp computer that I can't seem to get working right on the internet.

I have a broadband connection and a router. The other computer connected to the same router works fine.

I had the old version of Kerio (2.1.5) on both, I switched to the free Tiny firewall on the problem computer just to see if the firewall was the problem.

When I first start it it works fine. After a while I cannot connect to anything on the internet unless I reboot.

I am trying to set up the rules so that I block everything that doesn't need to connect to the internet.

One thing I am not sure of is something identified only as "SYSTEM" which looks like it wants to send and receive UDP traffic to the router and send and receive to and from the other computer.

Could blocking this be causing me to lose the internet

Re: Trying to Figure out What's OK and What to Block

connection?

I do not use the router as a way to network the two computers. I only use it to allow each computer onto the internet. So there is no logical reason for the computers to be talking to each other. Usually it says something to the effect that one computer wants to send a UDP datagram to the other computer on port 137. Should I allow this?

It's pretty easy to get lost in a nightmare of rules, popups and other nonsense when you try to control things like that. Since you're already covered inbound by the router, it would be better to just skip the software firewall and try using some common sense and keep any bad programs off the computer to begin with. Otherwise, you'll find yourself blocking normal things that need to communicate and the bad stuff will likely slip thru anyway. Best to keep it simple.

I agree with the philosophy of keeping it simple, but I have legitimate reasons for controlling the applications on the PC. For one thing, with Windows the "bad" stuff comes bundled with it. Take Windows Media Player. The first time you use it you set your preferences and prohibit the program from ever accessing the internet for any reason, not for updates, not to send information, not to obtain licenses, not for anything. And then ten minutes later the software firewall pops up and tells you that Windows Media Player is trying to connect to Microsoft for something. Without the software firewall you would never know.

You may say "so what," but my personal preference is that my video viewing habits remain private. Aside from that the program has some value. Occasionally it will play files that Videolan cannot. So I wouldn't get rid of it if I could, I just want to control it.

Another example is HP software that comes with their printers, scanners, etc. The only way I can stop it from sending out is to use a software firewall. Again, I just prefer that it doesn't connect out without permission.

As for trojans and viruses, I am careful about what I do, but who knows? With the firewall I can see if something new is trying to connect out and I can figure out what it is before I let it. It is just a little peace of mind.

As for the bad stuff slipping through anyway, that reminds me of the way some people say "why lock your doors? if they really want to get in they will." But if your doors are locked it is more likely they

Re: Trying to Figure out What's OK and What to Block

will look elsewhere for easier pickins.

BTW, some guy with an ip originating in China got past my router a couple of times – and hit the software firewall, which is how I knew about it. AFAIK it stopped there.

Ok, so you're basically one of those folks who isn't worried about the malware situation so much as which of your legitimate apps is trying to connect out and do what. There is some usefulness there I guess. I personally am not that paranoid or concerned. I could care less what Microsoft knows or thinks about my video viewing habits. I also could care less about most other programs phoning home. So for me, a simple cheap NAT router works fine with nothing else but an AV. And to be honest, if some program does things I don't like, then I don't use it. There are alternatives for almost every program out there, MS progs included.

If you want that kind of control over everything, then by all means go ahead and use Kerio or whatever, but that means you'll have to spend the time debugging your rules and finding out what everything does and needs in the way of IPs, ports and protocols, etc. So for you, some work is in store.. Good luck.

--

Kerodo

.