

What should I block out with my new firewall software?

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2004-02/1037.html>

From: Bob Ladbury (rladbury_at_kittymail.com)

Date: 02/14/04

Date: 13 Feb 2004 18:13:58 -0800

After much deliberation, it looks like I'm sticking to my good ol' Kerio Personal Firewall v2.15. I still don't know much about net communications, but I'm learning by entering configurations from people like SpongeBob. I'm wondering if there are major things I can block out that I don't use or need, like UDP or TCP. Reason I ask is that I believe I'm getting "pinged"; one of my rules is telling me that a couple of different remote addresses are trying to use XP's "Generic Hosts Processes for Win32 Services" at local ports 2265,2266,2267 through the TCP out protocol. At the same time, I'm also getting warnings I don't understand from XP's SYSTEM, UDP IN and TCP IN at ports 135-139. I got the W32 blaster worm yesterday that went through port 135, so for all I know, this could be local worm activity or attempts from outside hackers to penetrate these ports. Hence the reason I'd like to block ALL UDP and TCP, if I can get away with it, and tell Kerio to eliminate whatever other net services I don't need. I don't know what these protocols are used for, but here's what programs I use on my HOME system, that access the net:

- Web
- Email
- P2p
- occasionally software that needs to be updated

What I DON'T use or want to use is:

- Microsoft's web updates
- local home networks
- file/printer sharing (already turned off)

...and a bunch of other stuff I can't think of. Do I need MS's "svchost"? It runs like a half dozen processes in the background, and really gobbles up memory and keeps bothering my firewalls.