

Re: What should I block out with my new firewall software?

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2004-02/1040.html>

From: NeoSadist (*neosad1st_at_charter.net*)

Date: 02/14/04

Date: Fri, 13 Feb 2004 21:21:39 -0700

Bob Ladbury wrote:

- > *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";*

In my opinion, pinging is no big deal. Say your internet address is 24.240.225.88, you should allow pings from 24.240.225.1 (your ISP's router), so that they don't terminate your connection thinking you've gone offline.

- > *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.*

Don't have a clue what that is -- go read online.

- > *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.*

TCP/UDP on ports 135-139 and 445 are file sharing for networking. If you're sharing your LAN with other windows machines, you should allow those only to and from your other machines. No one else, especially not internet IP addresses, should be trying to access those ports.

- > *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.*

Exactly.

comp.security.firewalls: Re: What should I block out with my new firewall software?

> *Hence the reason I'd like to block ALL UDP and TCP, if I can get away
> with it,*

I think you're confused. TCP and UDP are the internet backbone -- without them, there is no internet. You should block 135-139 coming from the internet, true, but services are based on ports. For example, without 53 UDP (which is DNS, or how your computer knows that www.yahoo.com is actually 66.218.71.94), you'd have a horrible day wondering why your internet doesn't seem to work.

I could send you a sample configuration, but you'd have to translate it from english to kerio lol.

> *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*

This is port 80 for HTTP, and port 443 for HTTPS (secure web sites). That, and find out what servers your ISP uses for DNS (UDP port 53) and add a rule allowing dns to and from only those servers (but HTTP and HTTPS can be allowed to/from any server).

FTP, by the way, (or downloading) is over ports 20-21 TCP/UDP (don't have time to explain it further).

> - *Email*

Depends on what kind of email. Web-based email is fine using HTTP and HTTPS. POP3 (incoming email) is 110 TCP, SMTP (outgoing email) is 25 TCP, and IMAP (special email) is 143 TCP I believe.

> - *P2p*

Peer to peer is a very dangerous thing to use. Not only because the RIAA is out hunting down copyright law violators (yes, copyright is the law), but more importantly most viruses/trojans/worms are spread this way. I mean, do you trust these anonymous people you're downloading from? I wouldn't if I were you.

> - *occasionally software that needs to be updated*

This would be HTTP/HTTPS/FTP (windows update, etc).

>
> *What I DON'T use or want to use is:*
>
> - *Microsoft's web updates*

? This is more of a "go configure the thing not to do it" than blocking, since it's using HTTP/HTTPS/FTP.

Re: What should I block out with my new firewall software?

comp.security.firewalls: Re: What should I block out with my new firewall software?

> – *local home networks*

This means you're the only machine at your house, right? If so, you can safely block ports 135–139 and 445 (blocking both tcp and udp versions of those ports, both incoming and outgoing).

> – *file/printer sharing (already turned off)*

This goes along with "local home networks"

>

> *...and a bunch of other stuff I can't think of. Do I need MS's*

> *"svchost"?*

This program sometimes accesses the internet for other programs, so I'd go online and read up on it. I usually just allowed it, so long as I did frequent virus scans and browser security checks.

> *It runs like a half dozen processes in the background, and*
> *really gobbles up memory and keeps bothering my firewalls.*

Then maybe you should let it do its thing. Try this: unplug or disconnect from the internet, delete all kerio rules, and then allow everything that svchost does while the internet is OFF. Then, plug the internet back in (or reconnect) and from there don't allow anything further for that program only.

--

Smoking is one of the leading causes of statistics.

-- Fletcher Knebel