

Re: ZA Conceptual Question

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2002-10/13028.html>

From: Steve (pearsons_11112@mindspring.com)

Date: 10/30/02

From: Steve <pearsons_11112@mindspring.com>

"David" <davidwnh@adelphia.net> wrote in
news:8yIv9.1419\$6g.189441@news1.news.adelphia.net:

- > *There is plenty you can do with the firewall settings.*
- > *Program controls will not by themselves control traffic to a server*
- > *application. The high security setting blocks incoming unsolicited*
- > *traffic. The program controls will not by itself open a port for*
- > *incoming unsolicited traffic. The program controls do not of*
- > *themselves know which ports a program needs. If you run a webserver on*
- > *port 80 for example you would have to use the firewall controls to*
- > *specifically open port 80 if you are in high security mode. You may*
- > *allow all access to it in the program settings, however it will not*
- > *receive incoming unsolicited traffic unless you open the port via the*
- > *custom firewall setting. The firewall controls give you much better*
- > *control over what is and isn't allowed. You can close ports to*
- > *incoming unsolicited traffic if you are running in medium security for*
- > *example via the custom settings. It is also via the firewall settings*
- > *that NetBios,ICMP, etc. default settings are set or overridden so that*
- > *you can customize each security level to your own needs.*

I get it now. I had forgotten that I had to open specific ports to TCP/UDP in the firewall to get the program controls to start alerting me. For incoming-initiated traffic, the firewall and program controls act in series, first the firewall filters by protocol/port, then the program controls filter by program for whatever gets past the firewall.

- > *Program settings allow control over incoming and outgoing traffic that*
- > *is "initiated from within". It will not override firewall settings*
- > *that block "unsolicited" traffic. This is the key that most miss. The*
- > *firewall rules are absolute with regard to unsolicited traffic. There*
- > *is a huge difference in the handling of incoming traffic that is*
- > *unsolicited and incoming traffic which is a response to your own*
- > *outgoing traffic. Unfortunately due to ZL's ignorance to the need for*
- > *good documentation, this is not apparent unless you thoroughly read*
- > *the somewhat lacking documentation. You have to really dig deep into*
- > *the documentation or run a server application to figure this out.*

Agree 100%. They need an additional tutorial that goes a little beyond "just turn it on, and it handles everything for you!". Returning emailed tech. support requests would also be a bonus.

- > *The firewall settings will also allow you to block all outgoing*
- > *traffic on a port in custom settings regardless of program settings.*
- > *This is feasible with certain protocols that normally use specific*
- > *ports on both ends of the connection (NetBios). That is why NetBios*
- > *access is controlled here. If you block it here it will override any*
- > *program settings that try to allow it. Since many programs chose a*
- > *somewhat random high port to initiate a connection from, it is not*
- > *usually possible to control a client program this way without*
- > *affecting other programs also.*

This has always seemed like a flaw to me when writing firewall filter rules (up until installing ZA I've been using the firewall in my DSL box). For example, accessing a remote SQLServer you need to open 1433 as the destination port and 1024–65535 as the source port. However, if you have anything listening in that range on your local box, say pcAnywhere, it would allow a custom program to come in on that port, using 1433 as its source port. To do the filter rule right it seems like you'd have to change the source port range to 1024–5630,5633–65535. Does this make any sense to you? Thx.

- >
- > *With the firewall setting on high security you are not blocking any*
- > *ports(Netbios,etc. aside) to user initiated traffic unless you*
- > *specifically block them in the custom settings. All it really does in*
- > *this instance is pass the control of user initiated traffic to the*
- > *specific program settings. You are not overriding the firewall rules*
- > *with program control settings, because the default high security*
- > *setting is not blocking these ports to user initiated traffic to start*
- > *with! The only instance where the program settings override the*
- > *firewall settings is if you allow unsolicited inbound on a port via*
- > *the firewall settings then block that traffic through the specific*
- > *program setting.*
- >
- > *Anything you block by firewall rules is ALWAYS absolute. You will not*
- > *override this with program settings. The high security setting alone*
- > *is just not blocking as much as you think it does.*
- > *Start thinking of ports as one part of an addresses instead of*
- > *doorways and you might just start to understand this.*

Letting program controls handle locally initiated traffic works fine for my particular situation, but good to know the above anyway. This was exactly the info I was looking for. Many thanks.

- >
- >> *| Hmm...that's not my understanding at all. Program controls allow*
- >> *| you to control both accepting and initiating connections (both of*
- >> *| which involve inbound and outbound packets). By default program*
- >> *| controls accept or reject without respect to port number, but that*

comp.security.firewalls: Re: ZA Conceptual Question

>> | can be tuned as well (I can't think of any use for this). So
>> | apparently there's nothing you can do with the firewall that you
>> | can't do with program controls. Perhaps
> the
>> | intent is just a convenient way to shut down a port regardless of
>> | the program involved.
>>
>> The firewall rules are absolute, unless program controls over
>> ride
> them.
>> By example, if you set firewall security to Low, you will only have
> program
>> controls operating within the firewall package. This will leave all
>> ports open to any incoming packets. If an incoming packet activates
>> a sleeping trojan, theoretically, you should get an outgoing program
>> permission box. However, if that trojan is "spoofed" to look like
>> another program, you may not get that box. Additionally, at Low
>> setting, you NetBIOS and shared ports are open and available as well
>> (assuming your OS is not configured
> to
>> close them). No setting within program controls can close those, or
>> any other ports (except with respect to specific programs). So, I
>> don't see
> how
>> just the program controls could be used as an effective firewall
>> setup.
> You
>> could control outbound fairly well with just that, but your inbound
>> would
> be
>> wide open.
>>
>>
>
>

-
- **Next message:** : "(no subject)"
 - **Previous message:** Michael Maxwell: "Re: New Tech Board !!"
 - **In reply to:** David: "Re: ZA Conceptual Question"
 - **Next in thread:** Steve: "Re: ZA Conceptual Question"
 - **Messages sorted by:** [date] [thread] [subject] [author] [attachment]