

Re: Security Newbie – DSNkong, Proxomitron, Kerio

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2003-11/0885.html>

From: sponge (yosponge_at_yahoo.com)

Date: 11/15/03

Date: 15 Nov 2003 01:57:36 -0800

On 14 Nov 2003 02:33:36 -0800, dantesdigest2@yahoo.com (Dave) wrote:

>yosponge@yahoo.com (sponge) wrote in message
news:<8d76ec03.0311131510.3f8b88ea@posting.google.com>...
>> On 13 Nov 2003 08:21:54 -0800, dantesdigest2@yahoo.com (Dave)
wrote:
>>
>> >Hi Everyone,
>> >
>> >Hope someone can help me. I'm new to this stuff and am struggling
>> >with accomplishing a couple of things.
>> >
>> >I've installed all that I listed in the subject heading and have
got
>> >it working. A big accomplishment for me! :)
>> >
>> >I'm still having a couple of issues:
>> >I can't seem to connect to my website's cpanel manager.
>> >www.mydomain.com:2086
>> >
>> >I can't seem to get my FTP programs to work. I use Dreamweaver
and
>> >Filezilla.
>> >
>> >I imagine these are simple to fix, but I've been struggling for
the
>> >last few hours and not having any luck finding the answer in the
>> >groups.
>> >
>> >Thanks in advance for any help you can offer.
>> >
>> >Cheers,
>> >
>> >Dave
>>
>> Did you use one of my firewall rulesets? If so, go into the rule

list

>> *(right click Kerio's icon, select Administration, then click the
>> Advanced button on the menu that comes up). Scroll towards the very
>> end (don't use the square up-down arrows to scroll, use the regular
>> Windows scrollbar.) Find the rules pertaining to whatever browser
you
>> use and highlight the one called (whatever) Out. For example, if
you
>> use Mozilla, click the one called Mozilla Out and click Edit. In
the
>> Remote Port field, you can either add in the ports you will use
(like
>> 2086), separated by commas, or you can just set this to 'any' port.
(I
>> do not recommend setting it to allow connection to 'any' port
because
>> a lot of spam sites use non-standard ports; however, I realize your
>> needs may differ.) Click Ok, then Apply in the next menu, and Ok
again
>> to get out of the config screen. Everything should work fine.
>>
>> *Sponge*
>> *Sponge's Secure Solutions*
>> www.geocities.com/yosponge
>> *My new email: yosponge2 att yahoo dott com*
>
>
>*Thanks Sponge!*
>
>*You're awesome for the amount of help you offer others. I can now
>connect to cpanel, but still cannot FTP.*
>
>*The strange thing is that even if I turn off kerio and proxomitron
and
>dnskong, I still can't ftp. I was able to perfectly before I
>installed all this stuff. When kerio is on I see that it is allowing
>Dreamweaver to call out, but it will still not connect.*
>
>*Any thoughts?*
>
>*Thanks again,*
>
>*Dave**

Firewalls and FTP don't get along. In fact, FTP is very antithetical to a firewall's operation. There are a lot of ways around this, though:

1. Use FreshDownload (<http://www.freshdevices.com/downfiles.html>) and create a rule in Kerio allowing it full access. Go into Kerio's Advanced (rule-list) menu by right-clicking Kerio, select

Administration, then click the Advanced button. Go down towards the bottom and click Insert (just make sure it's above the rule called "Block All".) Give it a name, select TCP/UDP, BOTH directions, and for application, find the installed application (it helps to run it first so Kerio knows it's there) and select it. Everything else in the rule should be left alone. (ANY local port, ANY remote port, action set to Permit, etc.). You should be able to FTP away, I recommend this method most, for a lot of reasons: Freshdownload, IMHO, is the best download manager on the market, and one of the few that is spyware-free and/or doesn't cost \$20 or more. Since it only runs on demand, you will lose very little protection.

2. You can temporarily shut down Kerio. This is the least-recommended method.

3. You can set whatever FTP program you use to Passive (PASV) mode. You can also create or modify a rule in Kerio, allowing that program access to ports 20 and 21 (TCP, BOTH directions, the rest leave alone).

4. If you need to FTP from your browser, simply go into Kerio's rule-list menu, find your browser, and set it as follows:

Rule name: <your browser name> Out
Protocol: TCP/UDP
Direction: BOTH
Local Port: ANY
Application: <your browser's location on disk>
Remote Address: ANY (or, if you FTP to the same IP or group of IPs, use either single IP or network/mask to select them)
Remote Port: ANY
Action: Permit

This is appreciably less secure than using FreshDownload, but better than shutting down the firewall. Unfortunately, FTP is always a security problem, no matter which firewall you use.

Sponge
Sponge's Secure Solutions
www.geocities.com/yosponge
My new email: yosponge2 att yahoo dott com