

## Re: wireless and router; security issue

---

*Source:* <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2006-08/msg00591.html>

---

- *From:* unstablemicrosoft <[unstablemicrosoft@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:unstablemicrosoft@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Mon, 21 Aug 2006 10:21:02 -0700
- 

Hi. Thanks for your answer.

You said: "use Windows native client to avoid issues like yours (and allow configuration with AD group policy ). "

Btw, I have disabled the Windows client for networking/establishing a connection with other microsoft computers (sorry, for the fuzzy description) and the fileshearing service of my network connection. (I have no use for that) It seems that at one time that was advised by Steve Gibson at [www.grc.com](http://www.grc.com), although I cannot seem to locate that advice on his site now. So I'm not sure if I can do do what you suggest without reinstalling these.

I have Windows XP Home Edition service pack 2.

What native windows client could or should I use ? I don't know what you are referring to. Btw, To be honest, I'm not sure that would be safer. I have equipment from Sitecom.

The firewall I have is McAfee firewall 7.x, not the corporate version. Once, a representative of McAfee claimed that it would be safer to configure my firewall in such a way as to "trust" my home network. (I have it configured as home network, which seems to be the appropriate thing to do). That would be safer than not to trust it ... On another occasion, during a chat with a McAfee employee I got a more ambiguous statement. I have a router (connected to my cable modem by wire), wirelessly connected to my computer, no other computers in that LAN. I would think, that instructing the firewall to "trust" my home network, would mean that the McAfee firewall would "trust" any data coming in through my router. That just doesn't seem a sensible thing to do. My firewall is working more or less, although (don't ask me how !) I sometimes get "attempts to established an unwanted connection" with IP and port number in my log of incoming traffic. Usually it seems benign, sometimes not. I don't understand how it gets through the firewall of my router, it has some kind of firewall ... (that's about all you can say about that!) according to several tests.

Maybe I shouldn't have bought the McAfee firewall and antivirus combo, but the antivirus is still pretty good.

"S. Pidgorny <MVP>" schreef:

Re: wireless and router; security issue

If your access point requires WPA-PSK, and your wireless client connects, then you are using WPA-PSK and therefore your traffic is protected. I prefer to avoid vendors' utilities and use Windows native client to avoid issues like yours (and allow configuration with AD group policy ).

As for the client firewall, some details would help. It seems like your firewall is doing what it is supposed to do (because it's logging traffic appropriately) but you're unsure about your configuration itself?

--

Svyatoslav Pidgorny, MS MVP – Security, MCSE

-- F1 is the key --

"unstablemicrosoft" <unstablemicrosoft@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message [news:B130146F-1CE5-4CD0-8704-C9212890994C@xxxxxxxxxxxxxxxxxxxx](mailto:news:B130146F-1CE5-4CD0-8704-C9212890994C@xxxxxxxxxxxxxxxxxxxx)

Hi. Since I recently have been studying networking in general, I understand WAN's and LAN's better now.

But I have a question about my own network configuration, about what something means, particularly with regard to safety/security, but also in a broader perspective.

I'll outline my configuration briefly: ISP is cable company, from cable/wall socket a cable goes to the cable modem, from there a cable goes to the sitecom router, there is a wireless connection, using WPA-PSK encryption, between that router and the adapter on my computer in a different room. No other computers or devices in my network.

This morning my computer crashed, and I decided to deinstall and then reinstall my wireless adapter (Sitecom).

This may not be clear to you or you may not understand it, but I've decided to omit irrelevant information.

When I reinstalled the software of my wireless adapter, I saw, on the software panel of the adapter, under profile setting, profile name and network name, that it said "Sitecom". Just that, nothing else.

Since my router uses wireless encryption, I then instructed my adapter to connect to the router, and I gave the adapter the WPA-PSK code it needed to establish a connection with the router.

After having done that, on the adapters software "panel", under profile setting, profile name and network name, it showed an entry called "sitecom",

Re: wireless and router; security issue

and another entry, under profile settings, profile name, name  
:"<infra-sitecom>", network name Sitecom. Network type: access point,  
channel  
N/A (although there was an active connection!)

I decided to delete both entries, and to reestablish the connection by  
choosing site survey, connect, and then I gave the WPA-PSK code. Virtually  
instantly, a connection was established. Now, under profile setting, it  
shows  
profile name <infra sitecom>, network name Sitecom. (Btw, it still stated:  
channel N/A, while there was an active connection!)

So only one entry, instead of the two I had previously.

I don't really understand these entries. Please keep my configuration in  
mind.

I didn't see any point in having two entries, and thought that the plain  
"sitecom" entry might pose a security risk, or that it at least was  
redundant.

So, can anyone shed some light on this ?

Is having <Infra Sitecom> as the only entry safe ?  
Or was the other entry, plainly called "sitecom" of some use to me ?  
Again,  
I don't understand this.

With this only entry, the wireless connection seems to work perfectly, and  
I  
have had it configured that way for many months.

Also, I configured my McAfee firewall 7.x as a home network, and  
instructed  
it to NOT trust my home network. Yet, mysteriously, I sometimes get log  
entries in the log of incoming traffic (described as "unwanted connection  
attempts", sorry, crude translation), although my router SEEMS to have a  
firewall, according to several tests. Is there any connection between this  
and what I stated in the previous paragraphs ?

Advice/insight appreciated.

Thanks.