

Re: What is broken:McAfee firewall or my router ????? Urgent, ple

Re: What is broken:McAfee firewall or my router ????? Urgent, ple

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2006-08/msg00191.html>

- *From:* unstablemicrosoft <unstablemicrosoft@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Wed, 26 Jul 2006 10:01:02 -0700
-

One more thing to add: I used the option of testing my firewall in the security center of McAfee.

I got: "Unable to Probe

The IP address requesting this page is different from the IP address of your computer. This indicates that your computer is behind a proxy or NAT. These devices allow you to access the Internet by relaying traffic, typically from multiple computers, through a single IP address.

We are unable to directly probe your computer, you should take comfort from this. You have that much more protection between your computer and the Internet."

"Steven L Umbach" schreef:

If your internet router is not configured to port forward any traffic to your computer's IP I really doubt that traffic not initiated by your computer is going through it particularly if it is supposed to do stateful inspection. Were the "alerts" for TCP, UDP or both??

Steve

"unstablemicrosoft" <unstablemicrosoft@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message news:2D482029-4B7A-4962-82F8-0082C4B54B05@xxxxxxxxxxxxxxxxxxxx

Hi. I apologize for the length of this, but I want this to be complete.

I am very annoyed. I recently bought McAfee's firewall 7.x and antivirus 10.x. Home version, not corporate. Dutch (The Netherlands) version.

My configuration: ISP is cable company, from cable (wall) socket connection
by cable/wire to my cable modem, from there a connection by a cable/wire to
my router, from there a wireless connection to the adapter on my computer,
which is in a different room. No other computers in network. Encryption

Re: What is broken:McAfee firewall or my router ????? Urgent, ple

Re: What is broken:McAfee firewall or my router ?????? Urgent, ple

WPA-PSK, long random key.

I have a Sitecom router with the adapter that goes along with it. For security reasons I will not mention the precise model (am i too paranoid ? better too paranoid, than not enough) I bought this one early this year or late last year. All tests that I have used, including the advanced port scanner at pcflank.com, the port scan at hackerwatch.org, shieldsup at www.grc.com, the sygate test, the test at auditmypc.com, indicate that the router has a perfectly working firewall. It stealths some ports, while for as

far as I know McAfee does NOT do that. After using these tests, the probes

of these tests did not show up in the events log of the McAfee firewall 7.x

That means they did not get past the firewall of my router (Please keep my configuration in mind !).

Shortly after installing the firewall 7.x (I had 6.x) for the first time I examined the events log, and noticed at least one event. I wondered how that

was possible. McAfee said it was a router issue. I decided to disconnect the

router from power/electricity from a short moment, reconnect it and when it

was ready I reinitialized the router by pressing a "button" on the router.

I reestablished the wireless connection, gave everything the proper settings,

for security reasons I disabled the VOIP option, UPNP etc. I have disabled the option to control the router from over the internet.

I also configured the firewall for a home network, and configured it to not

to trust the home network. But that was not something new.

Yet, mysteriously in my events log (maybe it's called a bit different in English) it shows over the past three days that at least 8 times the McAfee

firewall met a probe, an attempt to establish a connection.

Hackerwatch.org

says that most these are probably hacking attempts. One "event" even had the

name trojan in it. And using a WHOIS on one other probe clearly indicated that it was a hacking attempt.

How is that possible ? I HAVE NO CLUE.

My networking gear notices one other wireless network sometimes, but there is very little wireless traffic around here. And seeing the IP numbers, the

names that go with the IP numbers, I find it hard to believe that this was

Re: What is broken:McAfee firewall or my router ?????? Urgent, please done wirelessly. But Maybe I'm wrong ? For as far as I know, they'd still have to deal with a long (random) WPA-PSK key.

SO, BASICS: WERE THE ATTACKS DONE WIRELESSLY ?
(UNLIKELY, SINCE I HAVE TRACKED/TRACED SOME OF THEM INTO THE USA) IF NOT, THEN, SINCE THE ONLY OTHER WAY TO CONNECT TO MY COMPUTER AND THE MCAFEE FIREWALL IS TO GO THROUGH THE FIREWALL OF MY ROUTER FIRST, AND ACCORDING TO TESTS THE HARDWARE FIREWALL WORKS FINE, AND WHEN TESTING MY COMPUTER THE TEST-PROBES NEVER REACH MY MCAFEE FIREWALL.

I contacted McAfee, they said it was a router issue, but that contradicts with what I have stated before. They started blabbering about that I was safe because the McAfee firewall blocked these attempts, probes, that I was safe because I reported to hackerwatch.org. They just seem to have no clue.

About contacting the manufacturer of my router: by email it takes ages, and on at least two occasions when I had sent an email they made statements that were nonsense. Calling on the telephone is very expensive. What can they do ? Especially because the tests indicated that the firewall in the router was all right, nothing. They won't give me my money back. And I don't think it's router issue.

A not properly working router firewall (cannot be turned off!, at least not by the instructions I once received) with just a McAfee firewall is just not good enough. I want both. What's going on with the firewall and the router ?

Just switching to a different firewall would usually not work, I'd probably have to remove all McAfee software, and deinstalling and reinstalling that would be problematic. You need (sometimes?) all sorts of tools to completely remove all traces from the previous installation. A Zonealarm/Zonealert firewall with McAfee antivirus is impossible, at least McAfee antivirus or the security center would object.

Also, I have the Spy Sweeper from Webroot, and the Spyware Doctor from

Re: What is broken:McAfee firewall or my router ?????? Urgent, ple

Pctools, updated, windows xp service pack 2 fully updated. For as far as I know, these programs did not detect the probes.

If you have any idea about what's going on, please inform me. I'd also appreciate it if someone could offer me a fix. Your help would be greatly appreciated.