

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/msg00280.html>

- *From:* "Steven L Umbach" <n9rou@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Wed, 26 Jul 2006 12:21:19 -0500
-

Blocked or stealth does not make any difference in my opinion and they both mean that the attempt to connect to your computer were either dropped or rejected. My guess is that most likely the traffic you saw was initiated by your computer regardless of what McAfee firewall said. If your router is port forwarding any of the ports you listed the firewall scans would have warned about those ports being available right away if you had any of those services enabled on your computer. If in doubt reset your firewall to default state but make sure it can not be managed remotely.

If your router/firewall is configured correctly then it should simply reject any TCP packet that has the syn flag set or does not have a matching sequence number. Syn means that another host is trying to establish a connection to your computer on a server service. To really find out if traffic is getting past your firewall you would have to run a packet sniffer like Ethereal on it without any software firewall enabled. To make it easier to find such traffic you could create an Ethereal capture filter to capture only TCP packets with the syn flag enabled. Ethereal is free and if you are interested the link below shows how to configure some popular Ethereal capture filters or you could simply fire up Ethereal when you are done using your computer to see what traffic is coming and going which should be minimal when you are not using the computer but still logged on.

Steve

<http://home.insight.rr.com/procana/> --- Ethereal capture filters

"unstablemicrosoft" <unstablemicrosoft@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message <news:F82FDFA3-7AD7-4567-927E-C92E9AF55C73@xxxxxxxxxxxxxxxxxxxx>

Hi. I appreciate any advice you can give me. I just reinitialized the router again and cleared the McAfee firewall's log, and I'll wait a bit and see if more shows up.

About port forwarding: I have not explicitly instructed the router or adapter do that. In my router menu it says under Port Fw. : Well known ports

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

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

: 7(Echo) 21(FTP) 23(Telnet) 25(SMTP) 79(Finger) 80(HTTP) 110(POP3). I believe that the router stealths at least the SMTP, the HTTP, Netbios and a

few others, according to several tests.

But these ports did not show up in my logs.

From the look of the menu it seems that (any other) ports and IP addresses won't be forwarded if you do not explicitly configure the router that way.

All the incoming "probes" were TCP, one UDP. Maybe something called eventlog, but I'm unsure about that.

Also, aside from some probes that were clearly hacking or scanning for hackable systems attempts, last night before I went to bed I received a large volume of incoming traffic, as recorded in the McAfee firewall's log, that seemed to originate from my ISP, or something that seemed to be associated with my ISP. (cable company)

Well, I contacted McAfee again, and after much conversation and waiting their message was that it must be a router issue, and they instructed me to contact the manufacturer of the router.

I contacted the manufacturer of the router, Sitecom, and what they said basically seemed nonsense. Please correct me if I'm wrong. But they have made statements in the past that turned out to be false. They said that I could receive data because that was necessary to be able to connect to the internet. I'm not quite sure if that statement even means that the router has a firewall or not. I did receive "probes" in the event log of my McAfee firewall that I had not asked for. One had even the name TROJAN in it. Nothing showed up in that log when performing some of the port tests mentioned below.

The router SEEMS to have a firewall, although this is not explicitly mentioned in the manual. I vaguely remember them saying in the past that the router has a firewall, although the word "firewall" is not shown in the software.

I then decided to turn off the McAfee firewall, and voila: the test shieldsup at www.grc.com showed that most ports were closed, a few were stealth. So, that must mean there is a firewall in the router ! Then how the hell did those probes get to my McAfee firewall ???

The advanced port scanner at PCFLANK.COM showed some ports as stealth, others as closed. A simple probe scan at hackerwatch.org showed some ports such as SMTP and HTTP as secure, "this port is completely invisible to the

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

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

outside world". Other ports were described as: closed but unsecure, "This port is not being blocked, but there is no program currently accepting connections on this port"

I'm basically writing this approximately chronologically, while trying to find an answer. Sorry for not writing a nice article.

I also tried a chat session with McAfee, but what could have been done in 2 minutes, took more than 20 minutes ! They can be so dense ! I asked a simple question: does the McAfee firewall have the ability to be "stealth" ? (almost certainly not), the other person often started making all kinds of assumptions about what my "real" question was, he contradicted himself, and at the end he gave totally incorrect information, then I was out of patience and ended the session.

I'm trying to make sense of all this. I'm fairly certain that the stealthed ports are safe. Or am I wrong ???

But what about the other ports ? Simple probe scan at hackerwatch said: not being blocked, but currently no program is accepting connections at this port. Would that mean (in what way??) that data can penetrate my router's (existing or non-existing) firewall ? Some things certainly showed up in McAfee firewall's log.

I turned my McAfee firewall on again, and tried the firewall test at auditmypc.com. Nothing reached the log of McAfee's firewall. What does it take to bypass my router's existing or not existing firewall ?? Maybe my concept of blocked, stealth, closed, and ??? is too limited. My router seems to have something called NAT, of the NAT services I turned off the VoIP pass through, thinking that might make a difference.

Do I have the worst router in the world ? it certainly wasn't cheap.

Please help !

"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

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

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

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

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

"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
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.

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

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 a 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 Pctools, updated, windows xp service pack 2 fully updated. For as far as I

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

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.