

Re: Do I need these services listening?

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2005-03/0759.html>

From: Gerald Vogt (vogt_at_spamcop.net)

Date: 03/15/05

Date: Tue, 15 Mar 2005 22:54:48 +0900

rodlinkowitz@whale-mail.com wrote:

> *Simply, the modem and router are –physically connected– to the first
> computer. The other computer (which I call the "client" or "secondary"
> computer) has only a cable attached to the first computer, hence it
> receives its internet connection via the first computer. Again, this is
> a standard configuration, nothing special being done here. I consider*

Sorry, but now you are contradicting your last message. Last time you wrote both computers are connected to the router and the router is connected to the modem. Now you are writing that there is no physical connection between the second computer and the router and the second computer is connected to the first computer (but how if the first one does only have one ethernet card?) So again, how exactly is your wiring?

> *the "server" computer as having both a public IP and a private IP,
> because it contains the router, which on one side (WAN) has a public*

Last time I checked a RP614 is a hardware device.

<http://www.netgear.com/products/details/RP614.php>

Your computer cannot contain that router...

The router does provide the internet connection. Not your first computer. The first computer and the second computer just use the internet connection of the router. Both computers are physically connected to the router by a ethernet cable. That's what it is supposed to be like. There is no need that the second computer receives its internet connection via the first computer. This is not possible unless the first computer is running Internet Connection Sharing which would be totally unnecessary as the router does already provide the internet connection.

> *address, and on the other side (LAN), a private one. But I believe the
> way you are looking at it, its the router that has the public address,
> and
> both computers have a private IP. (Note that servers completely outside
> my network can know about my LAN's private IP addresses, as exemplified
> in the test given at AuditMyPC, although this is done via javascript).*

comp.security.firewalls: Re: Do I need these services listening?

No, no server outside your network can know about your LANs private IP addresses unless you are using something that tells it to the outside, which may be a JavaScript inside your browser. Noone outside your router can send a packet to any of your inside IP addresses because the internal IP addresses are not routable and any router in between will just drop these packets.

- > *I'm convinced there is no one running a mail server on my system. But*
- > *the thing I'm not sure about is why, when I turned off ALL of my*
- > *firewalls on both computers, including*
- > *the SPI on the router (and even opened up the feature in the router's*
- > *setup to allow "pings"), I still got a solid wall of green (stealth)*
- > *blocks at GRC's ShieldsUp. Those include*
- > *the 25,110,445,135-139 ports btw, that were supposed to be "listening".*
- > *My only guess is the router's NAT feature, which can't be turned off,*
- > *is acting like a full on firewall. None of the other online security*
- > *tests I tried were able to penetrate the system either.*

NAT, when active, has many characteristics of a firewall although it is technically not one. Therefore, all the ports are supposed to be closed when scanned from the internet.

- > *Yes, correct. I think that may answer the question. At least two*
- > *software port scanners reported these two ports open, regardless of*
- > *whether I asked them to scan my public IP or my private IP. But NONE of*
- > *the online scanners showed*
- > *ANY ports open on my system. Maybe you should download a copy of*
- > *Advanced Port Scanner, try it on your system, and see what its telling*
- > *you! It might shed some light for you about how it works.*

I prefer not to install some software that I don't need on my computer, in particular when it comes from Russia... Anyway, the relevant scans in respect to security from the internet are the online scans. Those should show no open ports.

That a software scan of your public IP shows open ports inside the network, however, seems not correct. But at this time I won't try any more guessing until I fully understood your configuration. Under normal circumstances the scan of your public IP address would scan the router from the inside which may show some open ports in particular port 80 if the router does have a web management interface. The router should not have open ports 25 or 110, though, as it is not running a server.

- > *Okay, but can it hurt to block those ports I mentioned (135-139,445) on*
- > *the Netgear, or should I return it to default and just let NAT do its*
- > *thing? Maybe its purely psychological, but it makes me 'feel' more*
- > *secure to block those ports completely on the router's WAN*
- > *configuration as I did, as well as having the router block it via NAT,*
- > *not to mention its SPI, as well as having my 4 or 5 personal firewalls*
- > *block the ports as well. How else can I sleep at night?*

comp.security.firewalls: Re: Do I need these services listening?

You can block them on your Netgear. No problem there. But why do you have 4 or 5 personal firewalls on two computers?

- >> *one tiny piece: the web management interface on port 80 or 443*
- >
- > *depending*
- >
- >> *on your router and if it uses HTTP or HTTPS.*
- >
- > *And also the mail ports perhaps?*

I don't know the Netgear router. Under normal circumstances I would say, no. The Netgear should not have an SMTP server let alone an POP server running.

- > *Well I tried it on my two private IP addresses and same result: screen*
- > *goes blank for a few seconds, and then the command prompt returns. But*
- > *no error message,*
- > *no message of any kind.*

This is weird. That means that there is actually something listening on these ports but just closes the connection again after a few seconds. If there is nothing running you would get an error message. (Try "telnet 192.168.1.2 1234" with 1234 a random port that noone is listening to for comparison...) This is not good. But right now I am more confused about your configuration that I don't know where the problem could be.

Maybe you could write the output of the "ipconfig" command on both computers. That should clarify a lot about your setup with the Netgear.

Do you have a anti-virus with e-mail scanner running? Do the open ports still appear on your computers if the e-mail scanner (inbound and outbound) is turned off?

Gerald