

Re: Do I need these services listening?

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2005-03/0745.html>

From: Gerald Vogt (vogt_at_spamcop.net)

Date: 03/15/05

Date: Tue, 15 Mar 2005 14:34:29 +0900

rodlinkowitz@whale-mail.com wrote:

> Well, that's exactly how my system is set up. Each computer has one NIC
> card, the modem is plugged into the Netgear's WAN port, and each
> computer is plugged into the router's LAN port via Cat 6 cable, as well
> as their own NIC card. I may not have used the 'right' terminology
> perhaps to describe it, in previous posts. Of course, its only the
> first computer that has the modem & router, so I call the second one
> the "client". I do not use ICS and have no need to, and as is standard,

This is what I don't get. The first computer does not "have" the modem & router. Both computers are connected to router. Both computers are the same then. There is no difference between them in this regard. What do you mean when you say "the first computer [...] has the modem & router"?

> both machines have a distinct private IP address, with the server also
> having a public address from my ISP.

This again is wrong. Your Netgear router should connect to the internet. Your Netgear router should have the public IP address. Your computers inside don't know anything about the external IP addresses. They just have their private addresses and the Netgear as gateway which does the rest for them. So I also don't understand what you mean when you write "the server also [has] a public address from my ISP". No LAN computer should have any public IP address.

Your Netgear: a public IP address like 65.93.190.160 and a internal one like 192.168.1.1

Your computers: exactly one internal IP address like 192.168.1.2
(gateway configured as 192.168.1.1)

Maybe the output of the command prompt tool "ipconfig" from each computer would help to clarify here.

> Well that's what I was thinking... but I figured (with my limited
> understanding of network security), that if the ports look closed even
> to an internal port scanner, they are for sure going to be inaccessible

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

This is correct. Accessible from the internet are only the ports that are explicitly opened on your router and then forwarded to an address inside your LAN where there must be a server running.

> *to the internet. The problem of course is when I configured my router*
> *to close*
> *open ports like 25 & 110, which the software scanners were saying were*
> *open to the net, I could*

The problem with 25 & 110 is that they should never ever be open in your scenario unless you are running an SMTP and POP3 server which you don't.

This is a problem in any case. It does not help closing ports anywhere. You must find out why these ports are open.

Am I correct to assume that the information about the open ports 25 and 110 are from a port scanner software that you have run inside your network. No external online scanner did report 25, 110 nor any of the other ones open? Just want to be sure.

> *no longer send or receive mail! But I also told the router to close*
> *ports 135–139 and 445, and so*
> *far, I can't determine any bad effects from this. My pc-to-pc*
> *connection still seems to work ok.*

The router does affect only the connections between the WAN and the LAN. The LAN itself is connected through a switch which generally just sends everything through. "Closing" NetBIOS ports on the router does not make any difference in respect to the LAN file sharing traffic.

Second, there should no need to "close" ports. By default your router does NAT which is technically no firewall/filter but still does something similar. It allows you to connect to the outside and tries to figure out which of the incoming traffic from the internet is related to a connection from you to the outside (i.e. is a response to your request) and which is just unrelated garbage or someone trying to probe your IP address. That latter is usually just dropped and that's good so. So by default any online scan from the internet should report no open ports which means they cannot find any open ports on your Netgear from the internet. Only if you explicitly forward a port from the internet to the inside, only then it can be open and only then if the inside recipient does actually run a server on this port, else it would just report the port as closed. So there should be no need to block anything by default.

If you explicitly block port 25 and port 110 you block *_all_* traffic to port 25 and port 110 in the internet (or in both directions, the details depend on your Netgear router). If you block them in your router, your computers inside cannot access your E-Mail-Servers (SMTP for sending and POP3 for receiving) anymore. Again, there should be no need to block here anything as long as online scans don't report open ports and if they do I would rather figure out why they are open instead

Re: Do I need these services listening?

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

of blocking something that should not be open in the first place.

- > *Some of the software port scanners I used include: Moorer Port Scanner,*
- > *PCSuperScanner, Free Port Scanner,*
- > *Super Scan 4, PC Scanner, Local Port Scanner and Advanced Port Scanner*

O.K. Now I understand better. ;~)

- > *the best free scanner I've come across). I AM able to scan my private*
- > *IP on the second (client) computer using*
- > *Advanced Port Scanner, by entering its IP address. I'm also able to*
- > *scan my public IP address with APS, and in*
- > *this case, it even tells me the proper host name of my ISP, which seems*
- > *to indicate it is scanning my system as*
- > *would an online scanner, via my public IP address. The results I get*
- > *however are no different than when I enter the*
- > *WAN IP address given by my ISP. Which is why I remain unsure as to*

I suppose you mean the WAN IP/public IP address compared to the private IP address scan of your first computer. The WAN IP address is the public IP address.

I know it may seem strange but there is a huge difference if you scan the public IP address from the inside or the outside. The router has two IP addresses: the public IP address assigned by your ISP and the internal IP address which is probably 192.168.1.1 on your Netgear. Both IP addresses go to your Netgear. Only the public address can be reached from the internet, not the internal one. The internal one can only be reached from the inside. The router does not know from which side – inside or outside – traffic comes. If you connect to your router using its public IP address from the inside, it notices that and considers this traffic as any other inside traffic. There should be no big difference except for one tiny piece: the web management interface on port 80 or 443 depending on your router and if it uses HTTP or HTTPS.

You usually connect to your router with your browser with something like <http://192.168.1.1/> I suppose. Try the public IP address instead, e.g. <http://65.93.190.160/> This also gives you the normal web management interface. If you try to connect to this URL with the public IP from the outside, the router will block that traffic and won't accept it.

So what you should compare is an online scan from the internet, scanning your public IP address which should belong to your Netgear and compare that to your inside scan of either the private router address or the public IP address. The latter one should report at least port 80 as open.

Anyway, if you really run the NAT router as gateway with NAT any online scan scans the router from the internet. Any scan from the inside on the public IP address or the internal router IP address 192.168.1.1 should both report the same and may have some open ports which should not bother you as long as they look closed from the online scan.

Re: Do I need these services listening?

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

You cannot scan you inside computer with an online scan through a NAT router unless the inside computer is configured as DMZ in the NAT router. A DMZ computer inside basically receives any traffic to any port of your public IP address. Do not configure any computer inside your network as DMZ unless you really do know what you are doing. I assume here that you don't have a DMZ configured.

- > *whether the open ports and listening services*
- > *can be "heard" from the net.*

O.K. I hope this is clear now.

- > *That's what I thought... except I do tend to worry about 135, because I*
- > *got hit by a WORM through that port, and if it needs to remain open, I*
- > *want to be sure there is no way it can be accessed by anything outside*
- > *my LAN. (To this*
- > *effect, I blocked off the port via my router, and have created rules in*
- > *my firewalls to further block it out).*

(I posted regarding the closing of port 135 at another place in this thread...) If you are behind a NAT router and an online scan does not show port 135 open than there is no need to worry because noone can reach the port from the outside. Only if you run some malware inside it could exploit possible vulnerabilities as the access is open inside your LAN. But if you have applied all the latest Windows security updates I think there should not be any (known) problems at this time.

- > *1110*
- > *1125 (these two ports are used by my anti-virus, Kaspersky)*
- > *epmap (port 135! Use for "DCE Endpoint Resolution" (whatever that is),*
- > *and also by*
- > *a number of WORMS!)*
- > *microsoft-ds (port 445 Used by "Microsoft-DS" (whatever that is), and*
- > *also by a number of WORMS!)*
- > *netbios-ssn (I believe this is port 139, and its necessary for*
- > *communication between the two machines in my LAN)*

O.K. That's good. If this is the current state of open ports, there should be no malware. These are normal ports. No port 25 or 110 here. You should be able to close 135 and 445 as I wrote elsewhere in this thread.

- > *Note that neither netsat or WIL list ports 25 and 110 (they don't show*
- > *up at all, neither as listening or open). It is only from the scan of*
- > *all 65535 ports with Advanced Port Scanner, that it told me the only*
- > *two ports open were 25 and 110. But as I said, when I tried to close*

O.K. Which IP address where you scanning? The external public IP address (which is the router) or the internal IP address of your computer?

Anyway, if it was the internal one I guess that APS has a problem with the Microsoft IP stack implementation. Older versions of Windows and

Re: Do I need these services listening?

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

netstat also reported non-existing server ports listening. These are called "phantom ports". I would say that APS (which I don't know) still reports the phantom ports while netstat does not. Microsoft fixed their netstat implementation I think with Windows XP (or was it XP SP2?). Phantom ports are generally some remainders from a previous connection. The connection has been closed. No one is listening there but still the status of these ports is "listening" somewhere deep inside of Windows. The check with telnet for instance gives you the real information (well, not really, because a server could as well just block your connection attempt, but if telnet gets a connection you definitively know that there is something running...)

> *these ports through the Netgear, I couldn't use my email (which is why I had figured would happen!). When I think about it, I don't see how I can close those ports off to the net, and still expect to send and retrieve email at will.*

You don't have to close them as long as they don't appear in an online scan scanning your public IP address of your netgear router. The netgear is the essential device here. For your computer, there is no need to worry about it as long as nothing is forwarded through your netgear. Blocking is not required as nothing is accessible on your netgear on these ports, it does not forward traffic inside, and (hopefully) your computer only shows phantom ports.

I think you may try to reboot your computer and then run the APS scan before doing anything else (in particular not checking your e-mails ;-).

I think a fresh rebooted system should have no phantom ports anywhere as they require AFAIK previous existing connections.

>> *telnet 65.93.127.22 smtp*
>
> *Neat. Another trick I didn't know about. Gotta thank you for your part in my education of net security, Gerald. Anyway, this didn't show anything, no message came up, it just returned to the command prompt. I*

But you did get an error message? And: you must try this with the internal IP address of your computer. With the public one you just checked your router. So something like telnet 192.168.1.2 smtp for your inside computers give you the information whether something is listening on your computer.

> *guess this confirms I'm not running a mail server! So should I be worrying about ports 135 and 445 listening?*

I don't think so but you can close them anyway...

Gerald