

Re: How did they get past my NAT?

## Re: How did they get past my NAT?

---

*Source:* <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2007-10/msg00035.html>

---

- *From:* Maniaque <[maniaque27@xxxxxxxxx](mailto:maniaque27@xxxxxxxxx)>
  - *Date:* Thu, 11 Oct 2007 00:47:32 -0700
- 

OK, thanks very much for the reply, although now I feel like I've been made to wear the donkey hat and stand in the corner of the classroom... :)

On Oct 10, 12:35 pm, "Sebastian G." <[se...@xxxxxxxxx](mailto:se...@xxxxxxxxx)> wrote:

Simply ask for it?

What do you mean by "Ask for it"? If I do that (from outside the network), I get no response, because there is no "Default host" set up behind my NAT, and no port forwarding for that port – if an explicit port forwarding has not been set up, how can a remote host "Ask for" that server? Is this something that is allowed by the average NAT but requires extra network programming skills?

Wait until it comes up?

But why would it ever come up? Why would that port ever be opened to the outside from that machine? The port is bound to the VNC server (so no other program on the desktop should be able to do anything with it, as I understand?), and not forwarded on the router, so there should be no reason for a NAT session entry pointing that port to the outside ever to be opened, right? (I certainly don't open VNC connections to the internet, despite my limited knowledge I am very aware that basic VNC communication is totally unprotected, both authentication and data)

## Re: How did they get past my NAT?

The safety of a NAT, as I understand it, is that remote hosts cannot access an internal address unless there is explicit port forwarding enabled, or the session is initiated by a host behind the NAT, is that not correct?

What about implicit forwarding, for example by protocol helper implementations?

Sounds interesting, what is this? Is this the sort of thing that can sometimes make regular "Active" FTP work from behind a NAT, where the firewall automatically sees the FTP control port communication and opens up/forwards the data port as required? If so, how could the router be convinced to do this for an arbitrary port? Is there some sort of standard for triggering this behaviour?

I have just tested Active FTP from behind my NAT and it did not work (to an FTP server where passive FTP is working without issues) – does that say anything about this possibility?

I guess the questions are:  
– it is possible for a client TCP connection to be initiated by a local "client" program from a port that is already being used by a "server" program, like VNC server?

No, but using a protocol helper you can do this for a different port.

I've searched online for any information about "protocol helper", it seems to be synonymous with "IP helper" – I see a windows API, but that looks like it would require the attacker to be running arbitrary C/C++ code on the desktop (or other device on the network?). Do you know where I could find any information about what this is, how it works etc?

Assuming that the timeout for the NAT table entries is five minutes, it could be a completely different source.

OK, I'm going to show my complete lack of understanding about how NAT works here (if I haven't already :)), but it's the NAT device keeping track of the IP addresses (and some additional "magic" session information?) at both ends of the communication? What happens if two

Re: How did they get past my NAT?

## Re: How did they get past my NAT?

client machines try to open a connection from the same client-side port at the same time, does the NAT simply refuse one of them? I was under the impression that there could be multiple machines communicating to/from the same port from behind a NAT without problems. For that to be true, the NAT device would need to be looking at each incoming packet and sending it to the correct internal host based on some filtering logic, right (rather than a simple temporary port-to-host mapping table)? Are you saying that some arbitrary third-party IP address can send in a packet and have it be routed to a specific host behind the NAT, as long as the attacker has seen one of the packets of the communication between the legitimate remote host and the local host behind the NAT?

If I understand what you are saying correctly, and a remote attacker can actually direct arbitrary packets into any Existing NAT session by spying on a legitimate packet destined to/from the NAT-ed host, that still doesn't explain how the port session could be opened on the NAT device in the first place – is this where you are saying that the "Protocol Helper" comes in?

I'm very much counting on the fact that only specific selected ports should be accessible from outside.

Then implement this concept.

So... given that my ADSL connection uses PPPoA (which is non-bridgeable I believe, as opposed to PPPoE), I would need to set up a second router/firewall/NAT device like a linksys wrt54G to sit behind the telecoms-operator-provided Xavi router, forward the appropriate ports through both devices, and make sure that the firewall is turned on on the wrt54g? I can only assume that what was "missing" in my original setup was a firewall (which my adsl router claims to have, but when I turn it on all the port forwarding stops working, which sort of defeats the purpose). Or do you have any other suggestions on how this can be done using home equipment?

In theory, if any port on the desktop can be exposed, then my windows filesharing setup is just one of the things that would be vulnerable to brute-force attack.

Or DoS attacks.

## Re: How did they get past my NAT?

Meh, I'm not so concerned. Why would anyone bother? I'm a home user, I'm running a silly little website with 10 pageviews/month, my only concern is that someone gets into my machine / network and installs malicious code, spies on me, enlists my computer into a botnet of some sort, turns me into an infection vector for some or other virus / worm / trojan, etc. That would suck. It is incredibly unpleasant to have your desktop suddenly taken over via VNC, too, although I don't think that can happen again in quite the same way, I did upgrade away from the defective RealVNC version.

Is there anything else I can do to investigate this or help prevent future issues? Does anyone have any experience with the Xavi router or GlobespanVirata chipset that could help me get it set up to prevent this from happening again?

Maybe, but unless you know the implementation....

Not sure what you meant here – I know exactly how I have everything set up, but I don't know much about the workings / functionality of the router itself. There are no configuration manuals online or anything. In fact, I was able to get it to forward logging info to a syslog server on my desktop by browsing through and editing the "configuration backup" file, but afterwards remembered what I'd read a few months ago on some forum – you have to turn logging off on this router, because otherwise it hangs when it runs out of log space. No cycling, no "forward to syslog server but do not store locally", it simply hangs.

So it looks like at an absolute minimum I'm going to need to set up the second-level linksys wrt54g firewall/router, but I guess I'd like your criticism if you have any thoughts on the sensibleness of this idea, and whether it helps to "implement this concept" as you suggested above :)

Thanks so much for the feedback!  
Tao

.