

Re: Zoom ADSL Modem/Gateway

Source: <http://www.derkeiler.com/Newsgroups/alt.computer.security/2004-12/0252.html>

From: Mark (*kilroy_at_removethis.beer.com*)

Date: 12/10/04

Date: Thu, 09 Dec 2004 23:59:04 GMT

Jennifer wrote:

> *Thanks in advance for the help...*

>

> *I've been running a simple DSL-based home network with a basic DSL modem*

> *running into a Linksys router supporting 5 PC's – some Linux, some Windows.*

> *With that configuration, I've always been able to run nmap, or any other*

> *port scanner, at standard speed (normal) settings. We routinely will*

> *perform full scans against our outside client's networks – typically 35–40*

> *IP's at a time.*

>

> *We've never had a problem with that scan traffic interfering with Internet*

> *activities (web surfing, etc) on the other machines in our network.*

>

> *Now, in the interest of consolidating devices, we purchased a Zoom ADSL*

> *Gateway (5554) and replaced the modem and Linksys router. Everything works*

> *fine in normal traffic periods, however, whenever we attempt to run an nmap*

> *scan at anything above the –TI "sneaky" setting, Internet access across the*

> *network for all other machines grinds to a halt.*

>

> *I can't believe that a higher end gateway can't handle traffic that a basic*

> *modem/Linksys router can. I can find no settings or information related to*

> *any maximum number of connections or sessions that are supported by the*

> *gateway. Zoom tech support also confirmed that it shouldn't be an issue.*

> *Also, the unit only supports logging for system events and not for*

> *incoming/outgoing connections so I can't get any visibility into what's*

> *going on.*

>

> *Nmap is not sending out that much traffic, so is there anything else I'm*

> *missing? I'm about to return the Zoom and invest in a Netopia or something*

> *else more robust, but want to make sure I don't run into this issue again.*

>

> *Thanks –*

>

> *J*

>

>

I don't know the technical specs on that product and am having trouble finding much online. But, I have to wonder if it doesn't have something

to do with the DOS protection they mention. One thing vendors will do to try and prevent a denial of service attack is to limit the number of half-open connections. If that's the case then it's not a problem with the total number of connections, just the half-open ones.

Even at that, I would be surprised that it won't even allow 'polite' speeds. Anyway...

Out of curiosity, what type of scans have you tried? If it's just tcp (syn, connect) I'd be curious if the results are any different if you try a udp scan.

Later,

Mark