

Re: [fw-wiz] (no subject)

Re: [fw-wiz] (no subject)

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2006-06/msg00062.html>

- *From:* Frank Knobbe <frank@xxxxxxxx>
 - *Date:* Tue, 20 Jun 2006 13:12:08 -0500
-

On Mon, 2006-06-19 at 22:18 -0400, Paul D. Robertson wrote:

I've yet to meet a protocol designer who thought "Oh, people won't want to run my thing, I should make it easy to stop it."

Paul,

actually, I shouldn't have said protocol but setup or design. The issue here is not the protocol. The problem was:

"Does anyone have any ideas for blocking Google's new Google Talk client without blocking the Google web site? The IP addresses that the Talk client uses are the same addresses that resolve for Google."

So if the Google search engine and the Google Talk thingy use the same IP, and you can't block by IP the Talk stuff without affecting the Search web site, what does that tell you about their setup? Was this purely a coincidence, or was that **by design**? It seems it's the later. If Google Talk was using a different IP address than the Search Engine, the correct response would have been "Just block IP x.y.z.c". Instead the response was something more convoluted to filter name resolution.

Mind you, that was an authoritative answer from Google, not from some helpful soul trying to stop the Google talk. **That's** what caused a spray of coffee over the table.

That's been true of every new protocol in the last 6 or 7 years, if not longer. If you're going to let users install things, you're going to have to deal with it. Software restriction policies, ACLs, etc. You can't give up control of the end platform, then expect to get decent security by blocking arbitrary ports.

Again, that wasn't the point here. The issue was that Google is providing two types of services on the same address in such a way that you have to jump through hoops in order to disable one. I'm sure Google is large enough that they can afford more than one IP address. :)

Re: [fw-wiz] (no subject)

Re: [fw-wiz] (no subject)

But looky here! Today I get:

```
# host talk.google.com
talk.google.com is an alias for talk.l.google.com.
talk.l.google.com has address 216.239.37.125
talk.google.com is an alias for talk.l.google.com.
talk.google.com is an alias for talk.l.google.com.
```

```
# host www.google.com
www.google.com is an alias for www.l.google.com.
www.l.google.com has address 64.233.179.99
www.l.google.com has address 64.233.179.104
www.google.com is an alias for www.l.google.com.
www.google.com is an alias for www.l.google.com.
```

So it would appear that the initial reports are wrong and the IP addresses are indeed different. Hopefully you are able to block all distributed IP's for talk.google while leaving at least some for www.google unblocked so you can use the search engine.

And if that is still not possible, if Google makes it so hard to prevent access to certain services without affecting the search engine, then you can always just not use Google and use another search engine instead.

People seem to forget that they have a choice. They should resist getting wrestled into submission my mega-corporations. Sadly, most folks "go with the flow" and buy secondary and tertiary programs designed to keep faulty and broken primary programs running. They do whatever told by large corporations so that these can continue to profit.

But again, off topic. If no one sees something wrong with a vendor giving a lame-duck answer to a problem or challenge that is presented on purpose or by design, then perhaps ignorance is bliss.

Feel free to continue telling me how I should bow to protocols and just go with it since we lost the fight anyway. I won't :)

Cheers,
Frank

—

It is said that the Internet is a public utility. As such, it is best compared to a sewer. A big, fat pipe with a bunch of crap sloshing against your ports.

Re: [fw-wiz] (no subject)

Re: [fw-wiz] (no subject)

Attachment: signature.asc

Description: This is a digitally signed message part

firewall-wizards mailing list
firewall-wizards@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx
<https://listserv.icsalabs.com/mailman/listinfo/firewall-wizards>