

Re: Stateful Packet Inspection Firewall

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2003-02/1428.html>

From: NeoSadist (neos@dist)

Date: 02/13/03

From: "NeoSadist" <neos@dist>
Date: Thu, 13 Feb 2003 00:34:06 -0700

<greenNOSPAMaviator@bigfoot.com> wrote in message
news:21cl4vctis5q0a8dr0oos9ps97ansh3crt@4ax.com...
> *I just got a DSL Router which includes an SPI firewall. The
> manufacturer (Linksys) doesn't have very good technical support,*

I've never had a problem with them...

> *so
> I'm not much wiser as to how it works. The firewall screen has no
> configuration options which worried me first time I saw it.*

Why? Things that aren't tweakable worry you? Are you an
obsessive-compulsive?

>
> *In a previous message a few weeks ago someone said;
>
> >To over simplify it, SPI allows all of your
> >external ports to be closed until an internal request is made, then a
port
> >is temporarily opened for the response to that request only. This is
> >accomplished by using a state table.
> >If the firewall product you are using does not have stateful packet
> >inspection, then you are in the dark ages.*

That's an over-simplification.

>
> *Is this synopsis approximately correct, that connections are
> disallowed until the client initiates an outbound connection, or a
> "listen" on a port?
>
> Someone mentioned the following webpage;
>
> <http://www.sans.org/rr/firewall/anatomy.php>*

Then sans.org is correct, not the other person.

- >
- > *which again broadly says that SPI maintains a table for all*
- > *connections, and inspects packet contents for legality. My question*
- > *again is how "legality" is defined;*

By the firmware / hardware, obviously...

- >*whether anything that the client*
- > *computer initiates is treated as legitimate. My previous experience is*
- > *only with software firewalls i.e. ZoneAlarm, which blocks off incoming*
- > *ports but also controls which applications can access the net / listen*
- > *to ports. Presumably SPI does not place any restrictions on client*
- > *actions.*

Nope, but where's the rest of your trojan protection? Where's your antivirus? Where's your common sense (to keep you from installing "poisoned" software)? Where's your default hard disk permissions (win2k/xp)?

- >
- > *This is a bit worrying, because it seems to me that SPI places no*
- > *barriers in the path of a trojan that I might accidentally install*
- > *(from an email attachment say) on my computer.*

Yes, but if you aren't infected with one, what's to worry? Like I said, there are other layers of protection that are vital, not just the firewall, although firewalls are the "icing on the cake".

- >*If EvilTrojan installs*
- > *and listens on port 400 for portscans, how is the firewall to*
- > *differentiate between it and a legitimately written user application*
- > *which may also wish to listen on port 400? Linksys techsupport tried*
- > *to tell me SPI would prevent trojans, but they couldn't explain the*
- > *above point, and I think they're wrong.*

They are, to a point. It probably does it by not allowing outgoing on certain ports. However, yeah, SPI isn't meant for it. However, like I said, check the above rant on the "security has layers, ogres have layers".