

Re: Stateful Packet Inspection Firewall

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2003-02/1403.html>

From: DougNews (dougnews@Doesn'tWork.net)

Date: 02/13/03

From: "DougNews" <dougnews@Doesn'tWork.net>

Date: Wed, 12 Feb 2003 23:04:51 GMT

A little confusion on what you expect the router to do:

NAT is the process of setting up a table to keep track of outbound requests and allow answers back in. SPI is a process to inspect the packets coming in to ensure unwanted ones are not getting through – it will not stop viruses or trojans – just know cracker objectives. This site should help you – <http://www.smallnetbuilder.com/Sections-article18-page1.php>

So, you need a router with NAT to establish multiple machines to use one public WAN IP. An SPI firewall will help to keep out hackers/crackers and you will still need antivirus and possibly antitrojan products depending on your downloading practices. If you have a major concern, it also helps to keep a free software firewall running to watch outgoing connections as most routers are not application based but port based.

<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, 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.*
- >
- > *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.*
- >
- > *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;*
- >

comp.security.firewalls: Re: Stateful Packet Inspection Firewall

> <http://www.sans.org/rr/firewall/anatomy.php>

>

> 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; 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.

>

> 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. 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.