

Re: [fw-wiz] Post connection SYN

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2003-10/0120.html>

From: Paul Robertson (*proberts_at_patriot.net*)

Date: 10/17/03

To: Mikael Olsson <mikael.olsson@clavister.com>

Date: Fri, 17 Oct 2003 11:13:15 -0400 (EDT)

On Fri, 17 Oct 2003, Mikael Olsson wrote:

> *(sidenote: I don't think Raghuv eer was asking about syn flood
> protection, but rather prevention of SYNs in the middle of
> established TCP connections)*

Sorry, the phrase "Syn attack," along with some of the recent questions I've been looking at elsewhere had me thinking of SYN flood protection...

Out of state SYNs aren't really an "attack" per-se, dropping them is an artifact of stateful filtering, not a specific protection. However, as you point out, the receiving client isn't going to be able to deal with the packet anyway until it's timed out the original connection.

> *OR you set up the firewall to answer SYNs on behalf of the server
> and wait for the handshake with the client to complete before doing
> the handshake with the server, and assume that the firewall's state
> table can take much more of a beating than the server. Which is
> usually true. This way, you don't have to worry about rate limiting
> at all.*

You'd still want some sort of rate limit to stop floods and broken clients, unless you think a ring buffer solves that problem? Otherwise, you've just moved flood protection from N servers to less than N firewalls, no?

Paul

Paul D. Robertson "My statements in this message are personal opinions proberts@patriot.net which may have no basis whatsoever in fact."
probertson@trusecure.com Director of Risk Assessment TruSecure Corporation

firewall-wizards mailing list
firewall-wizards@honor.icsalabs.com
<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>