

# Re: Bad winsock behavior with SynAttackProtect and listen backlog exceeded

---

*Source:*

<http://www.tech-archive.net/Archive/Development/microsoft.public.win32.programmer.networks/2005-10/msg00320>

---

- *From:* "Alun Jones" <[alun@xxxxxxxxxxxxxxx](mailto:alun@xxxxxxxxxxxxxxx)>
  - *Date:* Fri, 28 Oct 2005 09:52:33 -0700
- 

"Tom Stewart" <[tastewar@xxxxxxxxxxxxxxxxxxxx](mailto:tastewar@xxxxxxxxxxxxxxxxxxxx)> wrote in message [news:eB13Ys72FHA.700@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:eB13Ys72FHA.700@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)  
> "The listen function is typically used by servers that can have more than  
> one connection  
> request at a time. If a connection request arrives and the queue is full,  
> the client will  
> receive an error with an indication of WSAECONNREFUSED."  
>  
> We started getting problems when customers implemented SP1 on their  
> Windows Server 2003  
> boxes. We'd see clients who thought they had successfully connected, but  
> who would get a  
> RESET back from the server immediately after the 3-way handshake (SYN,  
> SYN-ACK, ACK). This  
> seems \*completely broken\* to me.

Broken it may be – and it's certainly not what the TCP standards docs imply.

However, your clients need to accept that this behaviour may occur – and not just because of SynAttackProtect. If the client connects to a server that has chosen to bar their IP address, for instance, the TCP stack at the server will accept the connection before allowing the server's accept() call to complete, at which point the server will close the connection forcibly, resulting in the SYN, SYN-ACK, ACK, RST behaviour that you're seeing.

Note that there are many Windows TCP violations – my favourite, that I've been campaigning against (with no success) for over a decade, is that a full listen backlog queue causes a RST, when instead it should cause no traffic. (i.e. a SYN arriving at a socket that has all its backlog queue filled with connections waiting to be accepted, should be ignored – but Windows sends a RST incorrectly instead).

This is hardly one worth getting so het up about.

Alun.

~~~~~

[Please don't email posters, if a Usenet response is appropriate.]

Re: Bad winsock behavior with SynAttackProtect and listen backlog exceeded

—  
Texas Imperial Software | Find us at <http://www.wftpd.com> or email  
23921 57th Ave SE | alun@xxxxxxxxxx  
Washington WA 98072-8661 | WFTPD, WFTPD Pro are Windows FTP servers.  
Fax/Voice +1(425)807-1787 | Try our NEW client software, WFTPD Explorer.

---

- ***Follow-Ups:***

- ◆ ***Re: Bad winsock behavior with SynAttackProtect and listen backlog exceeded***  
◇ *From:* Tom Stewart

- ***References:***

- ◆ ***Bad winsock behavior with SynAttackProtect and listen backlog exceeded***  
◇ *From:* Tom Stewart

- Prev by Date: ***Re: connection failure: timeout***
- Next by Date: ***Re: Identify SAMBA Share drive***
- Previous by thread: ***Bad winsock behavior with SynAttackProtect and listen backlog exceeded***
- Next by thread: ***Re: Bad winsock behavior with SynAttackProtect and listen backlog exceeded***
- Index(es):
  - ◆ ***Date***
  - ◆ ***Thread***