

# Bad winsock behavior with SynAttackProtect and listen backlog exceeded

---

*Source:*

<http://www.tech-archive.net/Archive/Development/microsoft.public.win32.programmer.networks/2005-10/msg00313>

---

- *From:* "Tom Stewart" <[tastewar@xxxxxxxxxxxxxxxxxxxx](mailto:tastewar@xxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Fri, 28 Oct 2005 08:28:21 -0400
- 

Posted previously in microsoft.public.win32.programmer.kernel and microsoft.public.platformsdk.networking, and posting here now that I see this is a managed newsgroup related to networking

I'm going by years of experience and the following statement from the listen doc in winsock2:

"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.

After some research, this turns out to be caused by the new default of SynAttackProtect being enabled with SP1. The old, correct behavior (SYN responded to with RST when the backlog is full) can be restored by adding the parameter to the registry (HKLM\System\CurrentControlSet\Services\Tcpip\Parameters) as a 0.

I see that this was mentioned as far back as 2003:

[http://groups.google.com/group/alt.winsock.programming/browse\\_thread/thread/3008c02b84719c92/aad8c0e93a81a0a](http://groups.google.com/group/alt.winsock.programming/browse_thread/thread/3008c02b84719c92/aad8c0e93a81a0a)

so I guess the only new thing is the enabling of this behavior by default on servers.

Is there any hope of getting Microsoft to correct this errant behavior? A colleague's guess is that the way SYN attack protect is implemented involves trying to accept the connection, and it is only later discovered that the socket's backlog is full, so there's no place to put the accepted socket, so a RST is sent. While perhaps understandable, the external behavior is bogus.

So, assuming it can't (or won't) be fixed, this side effect desperately needs to be documented, both in KB articles that discuss SynAttackProtect and as a caveat in the listen documentation.

To summarize why this is bad:

## Bad winsock behavior with SynAttackProtect and listen backlog exceeded

- \* it breaks documented behavior;
- \* it gives a client app a false result from their connect call.

Hoping someone will do the right thing,  
—Tom

---

- *Follow-Ups:*

- ◆ **[Re: Bad winsock behavior with SynAttackProtect and listen backlog exceeded](#)**  
◇ *From:* Alun Jones

- Prev by Date: [Creating a protocol in hyper terminal application](#)
- Next by Date: [IoCompletionPorts with sockets question](#)
- Previous by thread: [Creating a protocol in hyper terminal application](#)
- Next by thread: **[Re: Bad winsock behavior with SynAttackProtect and listen backlog exceeded](#)**
- Index(es):
  - ◆ [Date](#)
  - ◆ [Thread](#)