

Re: Syn Attacks: Metabase entries (w3svc/ServerListenBacklog) & Backlog parameters

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.inetserver.iis.security/2002-12/6366.html>

From: Karl Levinson [x y] mvp (levinson_k@excite.com)

Date: 12/02/02

From: "Karl Levinson [x y] mvp" <levinson_k@excite.com>

Date: Mon, 2 Dec 2002 17:11:01 -0500

Your ISP may also be able to assist here. Also a good commercial firewall with Syn flood protection [netscreen.com 5xp starts at \$500, Checkpoint, Intrusion.com, Nortel Contivity switch, Cisco, etc.

<http://securityadmin.info/faq.htm#firewall>

"Ray Secrest" <res0cu5i@verizon@net> wrote in message
news:OcevrBkmCHA.2224@tkmsftngp02...

- > We are experiencing a large number of tcp connections (1500+) on our IIS 5
- > Web servers (SP2, SRP-1 & IIS Cumulative patch + many, many hot fixes) and
- > the servers will lock up. Our IDS has reported this as either a broken
- > network (the source originates outside our network) or a SynAttack. The IP
- > stack has been hardened as follows:
- > Tcpip/Parameters/SynAttackProtect 2
- > Tcpip/Parameters/TcpMaxHalfOpen 100
- > Tcpip/Parameters/TcpMaxHalfOpenRetried 80
- >
- > I was reviewing a few KB articles (Security Considerations for Network
- > Attacks & Q142641). While reading these I was trying to fully understand
- > some terms mentioned but I couldn't find them on TechNet or in Win2k
- Server
- > ResKit. What are the Backlog parameters, are they configurable and what
- are
- > the recommended settings? Is this related to the Metabase setting
- > W3svc/Server ListenBacklog (which is set to 1000)? The
- > W3svc/MaxEndPointConnections has been modified to 500 also.
- > Q142641 lists some parameters for WinNT 3.51 & NT4. Is it advisable
- to
- > use these on Win2k (heading in KB lists Win2k as applicable but Win2k is
- not
- > listed in body of article)?
- > Is there additional reading for these parameters (other than the
- RFCs)?

- > *Thanks*
- > *Ray*
- >
- >