Subject: Host/helo connection count exceeded - 346 - Should I worry

Posted by eastwood on Fri, 21 Apr 2006 00:09:54 GMT
View Forum Message <> Reply to Message

Just got my daily report

this figure seems very high, should i change some settings?

Never truly understand this part of the report

The traffic limiting is set up as out of the box settings as follows:

HostConnectionCount - Empty
HeloConnectionCount - Empty

Host NDR Connections - Empty
Helo NDR Connections - 1

Advice please anyone?

Subject: Re: Host/helo connection count exceeded - 346 - Should I worry

Posted by Heidner on Fri, 21 Apr 2006 06:35:08 GMT
View Forum Message <> Reply to Message

The large HOST/HELO count sounds a little like someone was either trying to relay mail through your box - or they were doing a dictionary attack trying to guess at email addresses for your network. I see that occasionally and they result is that they burn up bandwidth. For that reason I deliberately limited the number of HOST/HELO sessions that could be active. For me with a small network 15 or 20 inbound connections at any point is VERY HIGH. If you have turned on detailed and extended logging - you can see this as the session count climbs for example:

The large count could also becaused if a spammer is using your domain name as part of their return address for their spam. They fire off lots of garbage and your box is hit with all the Non-Delivery-Records that are reflected to your machine. Again another good reason to limit HOST/HELO connections, active HOST connections and HOST/HELO NDR connections.

Apr 17, 2006, 01:13:56 Session 2: 250-DSN
Apr 17, 2006, 01:13:56 Session 2: 250-SIZE 8192000
Apr 17, 2006, 01:13:56 Session 2: 250-AUTH LOGIN
Apr 17, 2006, 01:13:56 Session 2: 250 AUTH=LOGIN
Apr 17, 2006, 01:13:58 Session 3: (Delay Filter) Stop delay
Apr 17, 2006, 01:13:58 Session 3: (Delay Filter) Filter result is accept/deliver
Apr 17, 2006, 01:13:58 Session 3: (Spam Trap) No action
Apr 17, 2006, 01:13:58 Session 3: (Attachment Filter) From: "Sumerian D. Bravado"

Apr 17, 2006, 01:13:58 Session 3: (Attachment Filter) To: Dennis
Apr 17, 2006, 01:13:58 Session 3: (Attachment Filter) Subject: Try the new miracle weight loss herb
Apr 17, 2006, 01:13:58 Session 3: (Attachment Filter) Filter result is accept/deliver

I've never seen a session count above 5 for normal e-mail. But I have seen the count go quite high during dictionary attacks before I added limits... I doubled the typical session peak for ordinary emails and that limited my connections to 10. Small for many businesses. BUT in my case it helps throttle back the spammers.

I run a small network and have a small e-mail load -- so my settings reflect that... Since you've had NST for a while now... you should be able to take a look at your history from the daily reports or the logfiles and see if you are having an attack and/or adjust your limits..
