

## two strange issues...

**Source:** <http://www.tech-archive.net/Archive/ISA/microsoft.public.isa/2005-02/0325.html>

---

**From:** SSingleton (*SSingleton\_at\_discussions.microsoft.com*)

**Date:** 02/10/05

Date: Thu, 10 Feb 2005 12:59:02 -0800

I have two unrelated questions regarding my ISA 2004 installation. Here's our setup:

internal network is 192.168.x.x, Default setup rules for the Edge Firewall template allowing internal networks to access the net unrestricted, and two rules to publish web servers on the internal network.

### Question #1:

Twice over the last few days I've gotten an alert that one of the webservers has 'exceeded it's connection limit' and was disconnected. The alert mentioned the webservers internal IP address and told me to check the log. There were no other entries listed in the system or application log related to this subject.

Where in the heck do I set the connection limit for an internal IP. I don't think this is specifically caused by external connections coming through the publish rule, but maybe by some utilities that occasionally run on the web server to download data files, resolve IPs, etc. I'm not sure how to debug this problem.

### Question #2

When I look at the "sessions" I see a "secureNAT" session from an external IP Address. When I do a log query to look for activity from this IP Address I see that it's attempted a few SMTP connections to my SMTP publish. The SMTP server I use is a spam filter SMTP relay called ASSP. Anyway I checked it's logs and see that yes, it was logged as opening connections, but never transmitted any data. Unfortunately what I see is that those attempts happened over an hour prior to when I view this session in the session list.

A) why is that session still listed in the session list when it's not currently connected to my SMTP server, and hasn't been for over an hour.

B) why is it listed as a "SecureNAT" client in the session list when it's really an inbound SMPT packet? When I do a log query all the log entries show the proper rule which publishes the SMTP server. So Why the discrepancies in the Session list?

microsoft.public.isa: two strange issues...

--  
-Scott Singleton  
Alexandria, VA