

## Re: Spam Filter Causing ISA Alerts

---

*Source:*

<http://www.tech-archive.net/Archive/ISA/microsoft.public.isa.configuration/2007-12/msg00030.html>

---

- *From:* "Phillip Windell" <[philwindell@xxxxxxxxxxx](mailto:philwindell@xxxxxxxxxxx)>
  - *Date:* Mon, 10 Dec 2007 09:26:50 -0600
- 

Use the AD/DNS machines. How old they are is irrelevant.

"Matt" <[Matt@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:Matt@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)> wrote in message  
[news:8F0A6D43-64D9-4C6A-B8F2-69EF551926E0@xxxxxxxxxxxxxxxxxxxx](mailto:news:8F0A6D43-64D9-4C6A-B8F2-69EF551926E0@xxxxxxxxxxxxxxxxxxxx)

I have a Barracuda Spam Firewall and part of the way it works is to resolve DNS to ensure that emails are not coming from a fake domain.

That is a bad idea. It generates way too many look ups and the Barracuda has many many more ways to determine that something is SPAM. Use the other methods instead. A lot of the SPAM uses \*real\* Domains because the Spammers are smarter than that,...it is the Username part of the address that is fake and your lookups will not determine that. I also recommend that you turn off NDRs so the mail queue doesn't get clogged with worthless NDRs trying to go to fake addresses that will never happen,...you will have "good" mail get bottled up behind that and they will be waiting hours for their outbound mail to actually go anywhere because mail server will only send one message at a time in the order it hit the queue

internal DNS servers are old PII machines I set it up to look at my ISP's

DNS

server.

Use the AD/DNS machines. How old they are is irrelevant, they are doing DNS lookups, not rotating CAD graphics.

Now I can getting an alert in ISA that says, "The Non-TCP Sessions from One IP Address Limit Exceeded" If I acknowledge or reset the alert it will come back in five minutes or so. Is there a way I can tell ISA 2006 to allow these connections from that certain IP address? Thanks.

Re: Spam Filter Causing ISA Alerts

ISA MMC -->Monitoring-->Alerts Tab-->Configure Alert Definitions-->find Non-TCP Sessions from One IP Address....

Uncheck the box to disable it, or go into the details of it and edit the Specs. But I recommend you stop doing DNS Lookups to detect SPAM instead of screwing with the ISA.

--

Phillip Windell  
www.wandtv.com

The views expressed, are my own and not those of my employer, or Microsoft, or anyone else associated with me, including my cats.

---

Understanding the ISA 2004 Access Rule Processing  
[http://www.isaserver.org/articles/ISA2004\\_AccessRules.html](http://www.isaserver.org/articles/ISA2004_AccessRules.html)

Troubleshooting Client Authentication on Access Rules in ISA Server 2004  
[http://download.microsoft.com/download/9/1/8/918ed2d3-71d0-40ed-8e6d-fd6eeb6cfa07/ts\\_rules.doc](http://download.microsoft.com/download/9/1/8/918ed2d3-71d0-40ed-8e6d-fd6eeb6cfa07/ts_rules.doc)

Microsoft Internet Security & Acceleration Server: Partners  
<http://www.microsoft.com/isaserver/partners/default.asp>

Microsoft ISA Server Partners: Partner Hardware Solutions  
<http://www.microsoft.com/forefront/edgesecurity/partners/hardwarepartners.mspx>

---

.